ILIE TORSAN

CRIPTOLOGIE ELEMENTARĂ

-2007-

Chiar dacă prezenta lucrare nu este un îndrumar, un manual, sau o scurtă istorie a criptologiei, unele date şi informaţii de ordin general pe care le vom prezenta, le considerăm a fi de interes pentru cititor.

În perioada actuală asistăm la dezvoltarea fără precedent a ştiinţei calculatoarelor; tehnica electronică de calcul a înregistrat progrese imense, fiin larg utilizată în toate sectoarele, economic, ştiinţific, militar, administrativ sau social.

Ca expresie a unei nevoi crescânde de securitate generală, resimţită atât în sectorul guvernamental cât şi în sectorul privat, se acordă o atenţie din ce în ce mai mare, problemelor referitoare la protecţia INFORMAŢIEI, devenită resursă strategică de prim rang, atât în etapele de prelucrare şi stocare, cât şi în faza de transmitere.

Pe plan mondial aceste preocupări se concretizează în cele mai diverse forme: conferinţe tehnico-ştiinţifice pe profil, publicaţii dedicate în exclusivitate acestui subiect, introducerea în planurile de învăţământ ale unor institute de învăţământ superior a unor specialităţi strâns legate de tehnica securităţii datelor şi informaţiilor, apariţia unor firme specializate în probleme de protecţie şi securitate a sistemelor de calcul şi a informaţiilor etc. Nu lipsesc din rândul acestor preocupări cele referitoare la aspectele sociale şi juridice ale protecţiei informaţiilor.

În cadrul metodelor şi mijloacelor la care se apelează pentru soluţionarea acestor probleme, vizând protecţia informaţiei, CRIPTOLOGIA câştigă din ce în ce mai mult teren.

Se poate afirma cu deplin temei că astăzi Criptologia a intrat definitiv în marea familie a ştiinţelor, ea câştigându-şi statutul de ştiinţă particulară atât datorită domeniului propriu în care se manifestă, a metodelor şi

mijloacelor proprii, cât şi a înaltului profesionalism atins în soluționarea problemelor.

Aceasta înseamnă că toate atributele caracteristice fenomenului ştiinţific general se regăsesc şi în Criptologie, fapt deosebit de important deoarece pe această cale pot fi prevăzute direcțiile de dezvoltare şi se pot găsi modalitățile cele mai indicate de acțiune pentru realizarea scopurilor şi obiectivelor prezente şi viitoare ale Criptologiei.

Comercializarea şi democratizarea actului ştiinţific, valoarea lui estetică, sunt astăzi atribuite şi ale cercetării criptologice.

Ideile forță în Criptologie, dintre care unele au căpatat caracter programatic, apar în perioada premergătoare şi cea a desfăşurării celui de-al doilea război mondial, câştigând noi valențe în zilele noastre.

Dintre aceste idei forță prin care se manifestă Criptologia modernă, prefigurate în perioada amintită, reținem, printre altele:

- se cristalizează criteriile ştiinţifice de selecționare, încadrare şi pregătire a personalului;
- lucrul în echipe specializate, formate din reprezentanți remarcabili ai diferitelor specialități ştiinţifice, îşi demonstrează eficiența;
- apar colaborări între specialişti criptologi, aparținând diferitelor state, cu deosebire atunci când anumite interese politice, economice şi militare devin comune;
- infuzia aparatului matematic devine un element caracteristic, ajungându-se până la aprecierea că Criptologia a devenit o adevărată ştiință abia atunci când de problematica ei au început să fie preocupați în mod sistematic matematicienii, etc.

Dintre acei care, în perioada menționată, au contribuit la cristalizarea ideilor forță prin activitatea desfăşurată, amintim pe următorii, dintre miile de participanți pe acest front invizibil:

Germanul Werner Kunze, doctor în matematică a Universității Heidelberg, cu studii de fizică şi filozofie, remarcat în criptoanaliză încă din anul 1918, când reuşeşte să „spargă" unele Coduri aparținând Angliei şi Franței. Serviciul de criptoanaliză, denumit „PERS-Z", pe care l-a condus din 1936, a obținut rezultate deosebite. În 1945, când criptoanaliştii germani au fost capturați de armata americană, s-a aflat că ei şi-au înscris la activ decriptarea a numeroase cifruri şi coduri, aparținând un număr de peste 34 de state, în rândul cărora se aflau: Anglia, Franța, S.U.A., Japonia, China, Bulgaria etc.

Alături de Kunze s-au aflat doctorii în matematică Hans Rohrbach, Kothe Gottfried, fost vicerector al Universității Heidelberg, Rudolf Schauffler, bun cunoscător al limbii japoneze, preocupat de aplicarea teoriei probabilităților în criptoanaliză etc.

Artizanul intrării Suediei în frontul „spărgătorilor de coduri" este matematicianul Yves Gylden, profesor la Universitatea din Uppsala, avându-i alături pe matematicienii, Carl Segerdahl şi Arne Beurling.

Totodată Gylden a realizat o interesantă cooperare cu Norvegia şi Danemarca în acest domeniu.

Echipa poloneză care a reuşit să „spargă" prima variantă a maşinii germane de cifrat, tip ENIGMA, predând apoi modelul conceput acestui scop englezilor, avea în frunte trei tineri matematicieni, Marian Rejewski, Henryk Zuggalski şi Ierzy Rozycki.

Anglia a concentrat la Bletchley Park o forță ştiințifică de elită, formată din specialişti din cele mai diferite domenii, destinată activităților de

criptoanaliză. Din rândul acestora s-au remarcat, Alan Turing, renumit specialist în logica matematică şi precursor al calculatoarelor electronice, renumitul fizician Reginald V. Ioner, matematicienii, Oliver Strachey, Alfred Knox, Nigel Grey.

Despre activitatea şi reuşitele acestui grup, marele public a aflat abia în 1978. În semn de omagiu pentru succesele în criptoanaliză şi contribuția esențială la apărarea Angliei a lui Alan Turing, în 1978 s-a montat la Londra piesa de teatru „Breaking the Code" de H. Whitemore, avându-l ca erou principal pe Turing.

Încă din 1929, pe firmamentul criptoanaliştilor americani a apărut numele unui specialist de excepție, William Friedman, născut la Chişinău, apreciat ca unul dintre cei mai mari criptoanalişti contemporani, care prin activitatea desfăşurată în criptologia şi-a pus amprenta pe dezvoltarea acestei ştiințe în S.U.A. şi în lume.

Friedman a apelat cu prioritate la tinerii doctori în matematică, Frank Roulett, Solomon Kullback şi Abraham Simkov, dar şi la alți numeroşi specialişti, formându-se mai multe echipe de „spărgători de coduri", echipe care şi-au îndeplinit cu succes obiectivele propuse.

Dintre reuşite amintim „spargerea" maşinii japoneze de cifrat „A.T.–97", după eforturi deosebite care s-au derulat timp de un an de zile, şi codul naval japonez „J.N.- 25B".

O intensificare a cercetărilor şi aplicațiilor criptologiei, s-a constatat în momentul în care Criptologia a reuşit să spargă barierele impuse de sectorul guvernamental, ieşind de sub tutela exclusivă a unor organisme specializate; armata, ministerele de externe, poliția etc.

Asistăm astăzi la dezvoltarea aşa-zisei „Criptologii publice”, fenomen deosebit de interesant obiectiv necesar, încurajat în modalităţi diferite de organisme ale statelor, dar mai ales de către companiile particulare.

Ieşirea Criptologiei de sub tutela sectorului guvernamental s-a făcut şi se face, aşa cum este logic, cu respectarea anumitor restricţii, prima dintre acestea urmărind să nu fie afectată securitatea naţională a statului respectiv, restricţie care a generat şi generează încă ascuţite controverse între reprezentanţii statului pe de o parte şi reprezentanţii sectorului privat sau sectorului „civil”, pe de altă parte.

Rezolvarea corectă, constructivă a problemei şi deci a controverselor ivite este posibilă numai atunci când nu se acceptă din start nici totalitarismul guvernamental nici liberalismul uneori ireponsabil al sectorului privat, sau „civil”, atunci când reprezentanţii celor două tabere devin conştienţi că **„nevoile de securitate diminuează libertatea, dar fără securitate libertatea nu există.”**

Reţinem înaltul profesionalism cu care sunt abordate şi soluţionate problemele de Criptologie în sectorul particular, propaganda activă, organizată pentru însuşirea principiilor generale ale Criptologiei mai ales de către tineret. Această propagandă se realizează în principal prin publicaţii de specialitate, prin şcoli şi institute de învăţământ superior, prin reuniuni ştiinţifice naţionale sau internaţionale pe profil etc. dar şi prin practicarea exerciţiului criptologic în mod sistematic. Se apreciază că exerciţiul criptologic stimulează imaginaţia, perseverenţa, spiritul iscoditor, creativitatea, calităţi necesare tuturor celor preocupaţi de abordarea ştiinţifică a problematicii locului de muncă ocupat.

Întâlnim astăzi practicarea organizată a exercițiului criptologic de către studenții unor facultăți de matematică, ştiințe juridice şi chiar de medicină.

Un aport substanțial la apariția „criptologiei publice” l-au adus cei care în anumite perioade, mai ales în timpul celui de-al doilea război mondial, au participat direct la desfăşurarea acestor activități.

După trecerea unei perioade de interdicție, impusă de legislația țărilor respective, aceşti practicanți, în general remarcabili oameni de ştiință, au dorit să-şi prezinte activitatea, rezultatele obținute şi mai ales perspectivele Criptologiei. Referindu-se la un domeniu în general înconjurat de mister, lucrările lor au fost bine primite şi atent studiate, reținându-se din ele noi metode şi metodologii pentru asigurarea secretului datelor confidențiale, indiferent de sectorul la care ne referim.

Ca oameni de ştiință: matematicieni, fizicieni, chimişti, ingineri şi lingvişti, ei nu au omis să prezinte în aceste lucrări rolul ştiințelor respective în criptologie, oferind astfel colegilor lor un domeniu nou şi de perspectivă pentru aplicarea cercetărilor teoretice pe care le intreprind. Prestanța acestor autori, conferită de formația lor ştiințifică, avertizează pe cei care se vor „antrena” în acest fascinant domeniu că în Criptologia de performanță, amatorismul nu are drept la cetățenie, stimulând deci o abordare ştiințifică a problemelor, în concordanță cu importanța domeniului deservit de Criptologie.

*

* *

Luând în considerare utilitatea exercițiului criptologic, dar şi posibilitatea ca astfel de probleme sa apară în practica juridică, sau în activitatea de poliție, am întocmit acest material referitor la comunicările disimulate, deci la ascunderea unei informații confidențiale într-un text inofensiv, sau aparent inofensiv.

Sunt prezentate diverse metode de disimulare, fiecare problemă fiind urmată de soluția respectivă. Deci pentru a fi utilă această expunere, cititorul este îndemnat să citească problema, după care să treacă la rezolvarea ei, şi numai în caz de nereuşită să citească soluția care însoțeşte exercițiul.

Unele probleme sunt dificile şi tocmai de aceea satisfacția reuşitei este mai mare.

În partea a doua a lucrării, prezentăm câteva probleme referitoare la cifrurile de substituție.

Rezolvarea problemelor care vor fi propuse, va fi un alt prilej de satisfacție pentru cititorul interesat.

Cei care vor încerca, şi mai ales vor reuşi, rezolvarea problemelor prezentate în acestă carte, se vor convinge, chiar dacă numai parțial, de adevărul aprecierilor specialistului Ronald Lewin, confform căruia:
„Criptoanaliza nu este nici romantică, nici o chestiune de revelație imediată şi totală, ci este crearea cu extrem de multă răbdare a modelelor din bucăți care aparent nu au nici o legătură. Iar primul lucru pe care trebuie să-l găseşti sunt fragmentele.”

Cuvânt înainte

Considerăm util să definim pe scurt principalele noțiuni pe care le vom întâlni pe parcursul lucrării.

Criptologia este ştiința scrierilor secrete, având drept obiect apărarea secretului datelor şi informațiilor confidențiale, cu ajutorul sistemelor criptografice.

Criptografia este latura defensivă a Criptologiei, având drept obiect conceperea sistemelor criptografice şi a regulilor de folosire.

Criptoanaliza este latura ofensivă a Criptologiei, având drept obiect studierea sistemelor criptografice proprii pentru a le conferi caracteristicile necesare, astfel încât acestea să-şi îndeplinească funcția pentru care au fost concepute. Totodată criptoanaliza poate analiza sistemele criptografice ale terțelor părți, prin intermediul criptogramelor realizate cu ele, astfel încât prin „spargerea" acestora să obțină informații utile instituției pe care o deserveşte. Specialiştii din acest domeniu sunt cunoscuți cu denumirea mai romantică de „spărgători de coduri".

Prin sistem criptografic înțelegem o mulțime de transformări uniinversabile prin care mulțimea mesajelor (textelor) clare dintr-o limbă se transformă în mulțimea criptogramelor.

Considerații privind scrierile disimulate

Scrierile, sau mai precis, comunicările disimulate, sunt sisteme de comunicare în care o anumită informație este disimulată într-un text inofensiv, sau aparent inofensiv, pe baza unor conversații stabilite între corespondenți.

Metodele de disimulare sunt dintre cele mai diverse, şi ele depind de imaginația corespondenților. Se pot imagina metode de disimulare care sunt independente de textul purtător, precum şi metode care sunt legate într-un anumit fel de textul purtător, sau de o parte din el.

Dar indiferent de metoda de ascundere a unei informații confidențiale într-un text, operația induce unele modificări ale caracteristicilor statistice ale textului, specifice limbii române, textul ‚purtător" căpătând un anumit caracter „forțat". Identificarea acestor modificări, poate conduce, prin efort, tenacitate şi spirit de observație, la găsirea informației disimulate. Din acest punct de vedere, soluționarea unor astfel de probleme care solicită capacitățile intelesctuale ale individului, au o importanță practică imediată.

Deoarece astfel de comunicări se întâlnesc şi în mediul infracțional, specialiştii în ştiințele juridice ar putea fi interesați des tudierea lor sistematică.

Exemplele care vor fi prezentate, scot în evidență diversitatea metodelor de disimulare a unor informații.

La un astfel de sistem de comunicare – sau ceva asemănător – a apelat uneori şi Paul Rosbaud, spionul (în slujba englezilor) despre care se spune că l-a împiedicat pe Hitler să fabrice bomba atomică. Chimist şi fizician reputat, Rosbaud a ajuns rapid în cercul oamenilor de ştiință care lucrau la cele mai importante proiecte ale celui de-al doilea Reich, având legături în

toată lumea ştiinţifică internaţională, conducând prestigioase reviste de specialitate. Această ultimă funcţie îi permitea să transmită spionajului englez, prin intermediul unor articole publicate de diverşi autori în revistele la care era redactor, importante informaţii, evident fără ca autorii articolelor să cunoască acest lucru.

Iată un mod prin care Rosbaud ar fi putut comunica.

Să presupunem că într-o anumită revistă, un profesor publică o serie de articole de prezentare a capodoperelor universale. Începutul unui astfel de articol:

Romeo and Juliet

„In the ancient Italian town of Verona lived two noble families who were at deadly enmity with each other ...”

La sfârşitul articolului apare NOTA REDACŢIEI, care putea fi introdusă de redactorul şef, care era Rosbaud, notă având următorul conţinut: **„Ca o informaţie suplimentară, profesorul a răspuns solicitărilor, continuând să scrie despre capodoperele universale, găsind şi înţelegerea noastră. Pregătim chiar amplificarea reprezentărilor. Astfel de galanterii literare atrag cititorii. Restabilim sistemul sponsorizărilor, înlocuind vechile prevederi, operaţie necesară.”**

Destinatarul, cunoscând convenţia stabilită, procedează astfel: fiecare cuvânt din articol se înlocuieşte cu un număr, desemn-nd numărul de litere al cuvântului, şi obţine astfel şirul numeric, 2, 3, 7, 7, 4, 2, 6, 5, 3, 5, 8, 3, 4, 2, 6, 6, 4, 4, ...

Pe rând, câte un număr din acest şir, se scrie deasupra cuvintelor de ranguri impare (1, 3, 5, 7, ...) din textul care urmează după semnalul, NOTA REDACȚIEI, adică:

2 3 7 ...
Ca informație profesorul ...

şi din fiecare cuvânt se extrage litera care ocupă locul identic cu numărul înscris deasupra cuvântului respectiv. Cuvintele astfel extrase formează mesajul disimulat, adică, „A FOST CONTACTAT BOHR”.

Chiar dacă exemplul este ipotetic, informația presupusă a fi fost transmisă, este legată de un fapt real. Într-adevăr, fizicianul german Heisenberg, laureat al premiului Nobel în 1932, conducătorul cecetărilor germani care abordau construirea bombei atomice, l-a contactat pe savantul danez Bohr, laureat al premiului Nobel din 1922, cel care a elaborat teoria fisiunii nucleare, pentru a-l atrage la colaborare. Aflând de acest fapt, spionajul englez l-a răpit pe danez, ducându-l la Londra.

Dar să continuăm cu seria exemplelor.
Următorul text conține numele unui mare poet rom-n, pe care urmează să-l aflați:

„Evită să culegi cuceriri, abuzând de expresia – te iubesc frumoasă blondă”.

Extragem din toate cuvintele de rang impar din text, prima şi ultima lor literă, obținem succesiunea, EACIADEAICBA, din care, înlocuind fiecare literă cu rangul ei din alfabetul normal ordonat rezultă următoarea secvență numerică, 513914519321.

Din acest şir formăm alternativ numere dintr-o cifră şi din două cifre, după care, fiecare dintre aceste numere se înlocuieşte cu litera care, în alfabet, are acel număr drept rang, adică,

5	13	9	14	5	19	3	21
E	M	I	N	E	S	C	U

Următorul exemplu pune în evidență o altă modalitate de disimulare.

Să presupunem că un individ aflat în arest pentru cercetări, printr-un mijlocitor, îi trimite complicelui său următorul bilet:

Adormitule!

„Dacă nu obții nici un folos pentru cele concepute, pleacă unde este nevoie de un specialist cu studii universitare şi poate te susțin asociațiile umanitare”.

Chiar o sumară analiză statistică, ne conduce la concluzia că acest text are un caracter „forțat”.

Pentru început amintim faptul că, în limba română, cifrele pot fi substituite în mod unic cu literele inițiale ale cuvintelor care le denumesc, exclusiv 7, adică avem substituția,

1	2	3	4	5	6	8	9	0
U	D	T	P	C	S	O	N	Z

Lund drept bază primele şase litere, în ordinea descrescătoare a frecvențelor procentuale cu care apar în limba română şi comparându-le cu frecvențele lor în textul analizat obținem:

litere	A	I	E	R	T	N
fr. în limbă	13.8	12.54	11.79	7.89	7.42	6.16
fr. în text	8.66	13.38	14.96	3.14	9.44	8.66

După cum se observă, diferențele dintre frecvențe sunt semnificative, deci un prim semnal că textul are un caracter „forțat”.

În ordinea descrescătoare a frecvențelor ale literelor inițiale de cuvinte, primele şase litere din limba română, au următoarea ordonare, S, C, P, A, I, D, iar pentru textul analizat, literele inițiale de cuvinte au ordonarea,

U, S, N, P, C, D. Se observă că, în cazul textului, apar ca foarte frecvente inițiale de cuvinte, literele U şi N, care nu apar printre cele şase litere inițiale de cuvinte în limba română, în acelaşi timp lipsesc literele A şi I, care sunt frecvente ca inițiale în limbă.

Rezultă că această caracteristică statistică a limbii române este modificată în mod esențial în textul analizat.

În limba română, primele şase litere ca finale de cuvinte, în ordinea descrescătoare a frecvențelor de apariție, sunt: E, A, I, T, R, U, iar în textul analizat, aceste litere sunt: E, I, U, N, A, S, diferențele sunt evidente.

Din caracteristicile de mai sus, rezultă că textul analizat are un caracter „forțat", fiind suspect de a fi „purtător" al unei informații ascunse.

Dacă se extrag literele inițiale ale cuvintelor de ranguri impare dintext (primul, al treilea, al cincilea etc.) obținem succesiunea, DOUPCUNUCUPSU, observând că apar numai literele cu care se substituie cifrele în limba română, astfel că, pe baza acestei substituții, succesiunea de mai sus se transformă în următoarea secvență numerică: 2, 8, 1, 4, 5, 1, 9, 1, 5, 1, 4, 6, 1.

Dacă numerotăm literele cuvântului de adresare din bilet, obținem substituția,

1	2	3	4	5	6	7	8	9	0
A	D	O	R	M	I	T	U	L	E

în baza căreia, succesiunea numerică de mai sus, conduce la textul **„DU ARMA LA MARIA".**

Următorul exemplu evidențiază o altă modalitate de disimulare.

Să presupunem că individul A îi trimite complicelui său B, aflat în detenție, următoarea scrisoare, încercând să-l ajute într-o tentativă de evadare:

Dragă B, 1 februarie 19...

„Nu am găsit nimic rezonabil pentru Zina, va trebui să a aduc acasă în iulie sau august. Sunt puțin bolnav, ca orice om uitat dar am să încerc să lucrez, să caut să uit. Când vei ieşi, te angajezi ca remizier la Eugen, poate dacă ai treabă începi un trai normal."

Nu mai efectuăm analiza de la exercițiul precedent, ci vom trece direct la aflarea informației disimulate:

Literele cuvântului FEBRUARIE, le numerotăm în ordinea în care apar în alfabet, parcurgând cuvântul mereu de la stânga la dreapta.
Deci sub litera A scriem numărul „1", sub litera B numărul „2", sub prima literă E, scriem numărul „3", iar sub a doua literă E, scriem numărul „4" etc. Numerele astfel scrise formează permutarea (5 3 2 7 9 1 8 6 4).

Dintre cuvintele de ranguri impare, din fiecare frază (textul cuprins între două puncte consecutive) extragem literele lor inițiale. Conform celor trei fraze ale textului, obținem următoarele trei seturi de litere extrase:

NGRZTOAIA SBOUAILCU CIAREDTUN

Fiecare set se scrie sub permutarea aflată mai sus, după care culegem literele setului în ordinea naturală a numerelor din permutare. Astfel, pentru primul set obținem:

5	3	2	7	9	1	8	6	4
N	G	R	Z	T	O	A	I	A

din care, după culegerea literelor, rezultă secvența, ORGANIZAT.

Repetând procedeul şi pentru celelalte două seturi şi alăturând secvențele după culegere, rezultă informația căutată adică, „ORGANIZAȚI O BUSCULADĂ ÎN CURTE”.

Următorul bilețel conține o informație disimulată, printr-un procedeu foarte simplu.

„Sunt după masă la Eugen, ascultăm topul pe casetă. Te rog stai acasă, la revenire te caut, poate nu stau mult. La revedere, Nelu.”

Din cuvintele de ranguri impare extragem prima lor literă, iar din cuvintele de ranguri pare, extragem a doua lor literă şi obținem informația care a fost ascunsă „SUMA ESTE CERTĂ ARE CONT MARE”.

O altă metodă de disimulare se găseşte în exemplul următor.

Să se afle numele academicianului român, căruia îi aparține următoarea cugetare: **„Limba este întâiul mare poem al unui popor”**, ştiind că numele acestuia este disimulat în următorul text: **„Un ales poet, recunoscut eseist, încercat profesor universitar, bun dramaturg şi un filozof redutabil. A lăsat pentru admiratori o genială creație originală.”**

Evident că, informațiile suplimentare care sunt oferite de text, facilitază rezolvarea.

În acest scop, textul se împarte în grupe de câte două cuvinte consecutive şi, pentru fiecare grupă, numărul care exprimă lungimea în litere a primului cuvânt indică a câta literă din al doilea cuv-nt se va reține. Literele astfel extrase ne conduc la numele academicianului LUCIAN BLAGA, fost profesor universitar la Cluj, poet, eseist, dramaturg şi filozof, aşa cum este caracterizat şi în textul exercițiului.

Şi următorul exemplu evidenţiază o modalitate simplă de disimulare.

Să presupunem că asupra unei persoane aflată în cercetare – pentru a ne mentine în legenda adoptată – s-a găsit următorul înscris:

„Am avut succes cu organizarea taberei şcolare. În iunie organizăm tot noi aceste acţiuni, urmărind totodată relansarea întrecerilor elevilor la literatura universală. Să nu avansezi invitaţiile."

Analizând statistic acest text, se constată următoarele:
Frecvenţele procentuale ale primelor şase litere cele mai frecvente, sunt următoarele:

litere	A	I	E	R	T	N
fr. în text	15.75	12.12	10.9	9.69	8.48	7.87
fr. în limbă	13.80	12.54	11.79	7.89	7.42	6.16

Se observă abateri în cazul literelor, A R, T şi N.

Cele mai frecvente şase litere iniţiale de cuvinte în limba română sunt: S, C, P, A, I, D, iar în text ordinea este A, I, T, S, O, deosebirile sunt esenţiale.

Lungimea medie a cuvintelor în limba română este 4.50 litere/cuvânt iar în text obţinem 6.34 litere/cuvânt, din nou o abatere importantă.

Chiar şi numai aceste elemente sunt suficiente pentru a concluziona ca textul este purtătorul unei informaţii confidenţiale.

Cu puţină strădanie şi inspiraţie se ajunge la soluţie.

Se extrag literele iniţiale ale tuturor cuvintelor de ranguri impare şi apoi iniţialele cuvintelor de ranguri pare, rezultând informaţia căutată:
„A SOSIT AUREL SĂ ACŢIONAŢI LUNI."

Şi ideea din următorul exercițiu merită a fi reținută.
Presupunem că individul A îi trimite complicelui său, un bilet cu următorul conținut:

„Frica de Zina, care ştie totul, nu trece. Persoana strică tot. Fii atent la aviz, este un risc."

Cercetarea statistică evidențiază caracterul „forțat" al textului.

Mai mult, se observă că, tot a opta literă din text este o consoană, dar cum această constantă nu este o caracteristică statistică a limbii române, rezultă că ea reprezintă un „semnal" pentru corespondenți. Din această observație rezultă şi modalitatea de rezolvare.

Vom scrie textul pe coloane, fiecare coloană având opt litere;

F	I	T	N	E	T	F	L	T
R	N	I	U	R	R	I	A	E
I	A	E	T	S	I	I	A	U
C	C	T	R	O	C	A	V	N
A	A	O	E	A	A	T	I	R
D	R	T	C	N	T	E	Z	I
E	E	U	E	A	O	N	E	S
Z	S	L	P	S	T	T	S	C

şi din acest tabel reținem prima şi a treia linie, adică:

F	I	T	N	E	T	F	L	T
I	A	E	T	S	I	I	A	.

Citind aceste litere, încep-nd cu prima şi alternativ „sus-jos" obținem informația care a fost disimulată „FII ATENT EŞTI FILAT".

Legat de această modalitate de disimulare, prezentăm următoarea observație:

După cum se cunoaşte, data de 28 iunie 1883 marchează momentul îndepărtării lui Eminescu din presă, sa după cum apreciază Th. Codreanu, „înlăturarea" lui Eminescu de la făurirea destinului românesc.
După declararea publică a „gravei boli" care l-a atins „subit" pe Eminescu, fără ca boala să fie clar precizată, în numărul pe luna august a anului 1883 al revistei Literatorul, Macedonski publică următoarea epigramă:

Un X ... pretins poet - acum
S-a dus pe cel mai jalnic drum ...

L-aş plânge dacă-n balamuc

Destinul său n-ar fi mai bun

Căci până ieri a fost năuc

Şi nu e azi decât nebun

în care autorul traduce în versuri „boala gravă” prin nebunie.

La o analiză atentă se constată că, numărând şi litera „x” din primul vers, tot a şaptea literă din text este o consoană, fapt asemănător cu acela din exemplu precedent.

Considerăm atunci primele 56 litere din epigramă, scriem acest text pe coloane, fiecare conținând câte şapte litere, iar din acest tabel reținem primele două linii, împărțind literele respective în două blocuri, primul format din primele patru coloane, iar următorul din ultimele patru coloane, numerotând pentru fiecare bloc, coloanele. Deci obținem:

1	2	3	4	1	2	3	4
U	I	A	U	M	I	A	E
N	N	C	S	A	C	S	D

în care se observă poziția simetrică a literei A, în cele două blocuri, literă pe care o eliminăm.

Citind literele din cele două blocuri, începând cu primul, de jos în sus şi parcurgând coloanele în ordinea, 1, 4, 2, 3, obținem expresia „NU-S UNIC AM DECIS”, cu sensul **„nu-s singurul care am decis”**. Mesaj care confirmă faptul real că îndepărtarea din presă a lui Eminescu, la 28 iunie 1883, este rezultatul acțiunii unui grup de persoane din care a făcut parte şi Macedonski.

Următorul exemplu aduce în atenție problema verificării soluției obținute.

Să presupunem că individul A primeşte de la B următoarea telegramă:

„Presa noastră reproduce studiul despre posibilitatea întreruperii protocolului, presupunând totodată că neintervenția altor beneficiari încurcă numeroasele finanțări. Alin Spirache este mort."

Conform convenției dintre corespondenți, „cheia" de disimulare este dată întotdeauna, de ultimul cuvânt al înscrisului, deci în cazul nostru de cuvântul MORT.

Cu această „cheie", sau parolă, se proceda astfel: dacă ea are un număr par de litere, informația era disimulată în cuvintele de ranguri pare din text, dacă are un număr impar de litere atunci informația era disimulată în cuvintele de ranguri impare din text. Fiecare literă din parolă se înlocuieşte cu rangul ei din alfabetul normal ordonat, conform cu substituția:

A	B	C	...	P	Q	R	...	Z
1	2	3	...	16	17	18	...	26

În exemplul nostru, cuvântul MORT are 4 litere, deci informația este ascunsă în cuvintele de ranguri pare din text.

Înlocuind literele acestui cuvânt cu rangurile lor din alfabet obținem secvența, 13151820 din care se elimină zero, rămânând secvența numerică, 1315182. Câte un număr din această secvență se scrie deasupra fiecărui cuvânt de rang par şi apoi din fiecare cuvânt se extrage litera care se află pe locul indicat de numărul scris deasupra cuvântului.

Dacă este necesar, pentru cuprinderea tuturor cuvintelor de ranguri pare, secvența numerică, 1315182 se reia de la început. Deci avem:

1	3	1	5	...
Noastră	studiul	posibilitatea	protocolului	...

Literele extrase formează textul **„NU POT VENI.”**

Să presupunem că primitorul înscrisului nu-şi mai aminteşte cu exactitate care a fost parola stabilită, cuvântul MORT, sau cuvântul DECDAT, astfel că reia problema, considerând parola cuvântul DECEDAT. Având şapte litere, deci număr impar, va căuta informația în cuvintele de rang impar din text. Din parolă, înlocuind literele cu rangurile lor din alfabet obține succesiunea, 45354120, sau eliminând pe zero obținem secvența, 4535412 şi deci, din primul cuvânt extragem a 4-a literă, din al treilea a 5-a literă, din al cincilea a 3-a literă etc. Literele astfel extrase formează informația căutată, şi anume: **„SOSESC LUNI”**.

După acest rezultat, deruta destinatarului este totală, cele două informații sunt contrare. O soluție pentru rezolvarea enigmei, constă în a-i transmite emitentului întrebarea: **„Alin Spirache este mort sau decedat?”**

Un alt procedeu de ascundere, se găseşte în exemplul care urmează.

Unul dintre oamenii de ştiință, român, ar putea fi caracterizat pe scurt astfel:

„Dragoste pătimaşă pentru cercetare, îndrumător unic, generos, uman, profesor temerar preocupat de prestația tinerilor, om de omenie, un informatician neintrecut, considerat printre pionierii domeniului, umorist neegalat”.

Se constată că, literele inițiale ale tuturor cuvintelor de ranguri pare (2, 4, 6, ...)din text, sunt numai dintre acelea care substituie cifrele în limba română. Această constatare o interpretăm ca un „semnal” şi acest fapt ne conduce la rezolvarea problemei.

Textul se împarte în grupe de câte două cuvinte consecutive, litera inițială a celui de-al doilea cuvânt, prin cifra pe care o substituie, arată a câta literă din primul cuvânt al grupei se va reține.

Astfel, prima grupă este formată din cuvintele „Dragoste pătimaşă”, al doilea cuvânt începe cu litera „P”, substitutul lui 4, deci din primul cuvânt reținem a patra literă, deci pe „G”, etc.

Literele extrase conduc la numele savantului, GRIGORE MOISIL.

Şi următorul exercițiu aduce elemente noi, referitoare la posibilitățile de ascundere a unei informații confidențiale, într-un text.

Să presupunem următorul text transmis între doi corespondenți:

„Te rog să-mi scrii cât mai urgent, sunt nerăbdător să aflu ce ai realizat.”

În Universitate se aduc acuzații legate de matematizarea şi modernizarea predării, prin încărcarea şi prelungirea zilei peste capacitățile cadrelor, salariaților şi studenților. Uneori criticile sunt curmate, dar străinii văd prin câte încercări trecem.

Dacă analizăm statistic primul paragraf al înscrisului, se constată că el are toate caracteristicile unui text normal în limba română, deci este puțin probabil ca informația să fie disimulată în această porțiune.

Pentru partea a doua a înscrisului observăm următoarele:

Cele mai frecvente litere inițiale de cuvinte, au următoarea ordonare:

S, C, P, I, A, D, iar în limba română ordonarea este, S, C, P, A, I, D, deci avem identitate perfectă, fiind puțin probabil ca în această parte să fi fost disimulate literele informației confidențiale.

Acelaşi fapt se constată dacă se face statistica literelor finale de cuvinte.

Pentru frecvența procentuală a primelor şase litere, în ordinea descrescătoare a frecvențelor, obținem valorile:

litere	A	I	E	R	T	N
fr. în limbă	13.80	12.54	11.79	7.89	7.42	6.16
fr. În text	14.14	16.58	13.17	6.82	8.78	5.85

Deosebirile sunt importante, mai ales în cazul literelor, I, E şi R.

Pentru lungimea medie a cuvintelor din text, obținem valoarea 6, 54 litere / cuvânt, în timp ce pentru limba română acest indicator are valoarea, 4, 85, deci apare o diferență semnificativă.

Din aceste constatări rezultă că, cel mai probabil, literele informației confidențiale sunt însemnate în acest paragraf, cu precădere în cuvintele lungi.

Este nevoie însă de multă răbdare, tenacitate şi spirit de observație, dar şi de intuiție, până să se afle informația confidențială.

Pentru cei doi corespondenți lucrurile sunt simple, conform convenției ei procedează astfel:

Din primul paragraf, toate cuvintele care au cel mult 6 litere, se înlocuiesc cu numerele care exprimă totalul literelor lor, şi se obține secvența numerică: 2, 3, 4, 5, 3, 3, 6, 4, 2, 4, 2, 2, secvență care, dacă este necesar se reia de la început.

Din al doilea paragraf se consideră numai cuvintele care au cel puțin 6 litere (deci, 6, 7, 8, ...) deasupra lor se scrie câte un număr din secvența numerică de mai sus, după care din fiecare astfel de cuvânt se extrage litera care, în acel cuvânt, ocupă un loc identic cu numărul înscris deasupra cuvântului respectiv.

Literele astfel extrase formează textul: **„NU AM DECLARAT NIMIC”.**

Pentru puțină relaxare, iată un exemplu simplu.

Să presupunem că, individul A, aflat în cercetări, primeşte printr-un intermediar, următorul bilet de la un complice:

„Mama nu ascultă nimic. Însănătoşirea este urmare credinței, cinstei şi curajului ei.'

Soluția este uşor de obținut.

Din cuvintele de ranguri impare din text, se extrage din fiecare literele de pe locurile, 2, 3, 4, rezultând informația disimulată: **„AM ASCUNS ARMA ÎN ŞURĂ."**

Să considerăm cazul în care individul A primeşte două mesaje de la acelaşi cetățean B.

Fie aceste mesaje următoarele:

Primul mesaj: **„Sunt puțin cunoscut aici. Alex mi-a mărturisit la întâlnire unele aspecte grave."**

Al doilea mesaj: **„Nu cunosc aranjamentele. Reputatul meu medic oftalmolog pleacă. Amabil, respectuos şi plăcut, cum sunt românii."**

Având două mesaje, în care informațiile confidențiale sunt disimulate prin acelaşi procedeu, rezolvarea problemei este mai puțin dificilă.

În acest sens, suprapunem cuvânt cu cuvânt cele două texte:

Sunt	puțin	cunoscut	aici	Alex	mi-a	....
Nu	cunosc	aranjamentele	Reputatul	meu	medic	...

Şi vom încerca să formăm simultan cuvinte din cele două texte, cu condiția ca, din cuvintele suprapuse să folosim litere de acelaşi rang. Astfel, din primul text, şi primul cuvânt să considerăm prima literă, deci pe „S",

atunci şi din al doilea text şi primul cuvânt, vom considera tot prima literă, deci pe „N”. Comparând primul cu al doilea cuvânt, din textul al doilea, urmărim să vedem care literă din cel de-al doilea cuvânt se poate lua, astfel încât acesta, împreună cu „N”, din primul cuvânt formează o bigramă posibilă în limba română. Considerând toate literele din al doilea cuvânt, ar rezulta bigramele, NC, NU, NN, NO, NS, NC, fiind posibile numai, NU, deci când din al doilea cuvânt am luat a doua literă, pentru care în primul text rezultă bigrama, SU, respectiv bigrama, NO, când din al doilea cuvânt am luat a patra literă, rezultând în primul text bigrama, SI.

Să reținem cazul, NU, din textul doi, şi corespunzător, SU, din primul text, după care, în ambele texte trecem la al treilea cuvânt. În cazul primului text, pornind de la bigrama, SU, cea mai frecventă trigramă este, SUN, când din al treilea cuvânt am luat a treia literă, dar atunci în textul doi rezulta trigrama, NUA, care sub forma, NU-A formează un început de text frecvent în limba română, ş.a.m.d.

Din aproape în aproape se obțin informațiile disimulate, în primul text „SUNĂ LA MĂTUŞA”, iar în al doilea text „NU ARE DOLARI ACUM”. Regula de disimulare este „1, 2, 3” deci din texte se formează grupe de câte trei cuvinte consecutive, şi pentru fiecare, din primul cuvânt se reține prima literă, din al doilea a doua literă şi din al treilea cuvânt, a treia literă.

Un exemplu simplu, mai mult pentru relaxare.

Precizați care este „idealul politic” despre care este vorba în următorul text:

„Prin acțiuni inteligente şi degrevate de aparențele politice, idealul politic principal, învingând greutățile, devine barometru al capacității de adaptare”.

Soluția: **„INTEGRAREA ÎN EUROPA”**.

O idee nouă de disimulare a unei informații într-un text, se găseşte şi în următorul exercițiu.

Să considerăm următorul text, schimbat între doi corespondenți:

„Am auzit că te-ai însurat în mare secret.

Poate că tu nu regreți, dar cine te ştie, consideră viitorul tău statut cam pretențios. Vom sărbătorii la anul primul carnaval din istoria acestei instituții."

Conform convenției dintre corespondenți, pentru aflarea informației transmise, se procedează astfel:

În prima frază (începutul textului până la punct), vom nota pentru fiecare cuvânt, rangurile ocupate de vocale. Astfel, din cuvântul AM, rezultă numărul „1", din cuvântul AUZIT rezultă numerele, 1, 2, 4, etc. Continuând pentru toate cuvintele acest procedeu, obținem secvența numerică; 1 1 2 4 2 2 3 4 1 4 6 1 2 4 2 5.

Deasupra cuvintelor de ranguri pare, din textul care urmează în înscris, scriem câte un număr din secvența numerică de mai sus, număr care va indica a câta literă din acel cuvânt se reține. Literele astfel reținute formează expresia: **„TRIMITE BANII".**

Şi tot o noutate descoperim şi în acest exemplu, în care se cere descoperirea informației disimulate în următorul text:

„În această carte scumpă se impun orientului religii şi sisteme mai normale".

Să considerăm alfabetul normal ordonat, şi rangurile literelor în această ordonare, adică

A	B	C	...	P	Q	R	...	Z
1	2	3	...	16	17	18	...	26

Scriem numărul de litere din text, care se găsesc între literele N şi R, consecutive şi obţinem şirul numeric, 9, 14, 1, 2, 5, 18, 1, după care, fiecare număr se înlocuieşte cu litera care, în alfabet, are acel număr drept rang, adică

9	14	1	2	5	18	1
I	N	A	B	E	R	A

secvența finală, citită de la dreapta, conduce la informația căutată:

„ARE BANI”.

Astfel de scrieri disimulate se pot întâlni în cele mai diferite medii, aşa cum se va observa din următorul exemplu.

Să considerăm poezia lui Eminescu, „Şi dacă de cu ziuă ...”, scrisă în 1876 şi având patru versuri:

„Şi dacă de cu ziuă se-ntâmplă să te văz
Desigur că la noapte un tei o să visez
Iar dacă peste ziuă eu întâlnesc un tei
În somnu-mi toată noaptea te uiți în ochii mei”.

Aflați cum este disimulat în poezie, numele unei persoane dragi poetului.

Considerăm textul cuprins între cuvântul „văz”, din primul vers şi cuvântul „ziuă”, din al treilea vers, text pe care-l scriem ca un şir de litere, deci eliminând pauza (sau spațiul) dintre cuvinte. Deci

VAZDESIGURCALANOAPTEUNTEIOSAVISEZIIARDACAPESTEZIUA.

Din acest şir, reținem prima literă deci pe „V’ şi omitem următoarele trei litere, reținând litera care urmează, adică litera E, omitem următoarele

patru litere şi reţinem litera care urmează, adică litera R. Dacă scriem între paranteze literele (mai precis numărul lor) care se omit, şi notăm literele reţinute, algoritmul se scrie astfel,

V (3) E (4) R (5) O (5) N (7) I (8) C (9) A

A rezultat numele iubitei, **VERONICA** iar cheia de disimulare este **3, 4, 5, 5, 7, 8, 9.**

În exerciţiul care urmează se face apel şi la puţină matematică.

Să se afle informaţia disimulată în următorul text, ştiind că aceasta are legătură cu Eminescu:

„Cum s-a încălzit, începem pregătirile pentru concediu şi ne calculăm bugetul. În club totul este normal, nu am putut zugrăvi faţada. Las aşa dar la iarnă vopsesc totul alb."

Informaţiile suplimentare ajută la rezolvarea problemei, chiar dacă acest lucru nu este foarte uşor de realizat.

Să considerăm secvenţa numerică; 1, 2, 3, 5, 8, 13, 21, numită secvenţa fibonaciană, dat fiind faptul că aparţine şirului numeric al lui Fibonacci; 1, 2, 3, 5, 8, 13, 21, 34, 55, ..., a cărui limită este celebrul „număr de aur".

Din cuvintele care, în text, au rangurile egale cu numerele din secvenţa de mai sus, se extrag literele lor finale, după care secvenţa numerică se reia de la început, până se parcurge tot textul.

Literele extrase conduc la numele voievodului Matei Basarab, preferatul poetului Eminescu.

Dar să mai rămânem sub imperiul şirului lui Fibonacci, cu un exemplu, care aduce în atenţie rolul întâmplării în căutarea unor informaţii

confidențiale disimulate într-un text. Se poate întâmpla ca soluția găsită să fie rodul întâmplării, textul analizat fiind total inofensiv.

Exemplul nostru se refer la poezia eminesciană **„Somnoroase păsărele”**, mai precis la prima ei strofă adică:

„Somnoroase păsărele
Pe la cuiburi se adună
Se ascund în rămurele
Noapte buna!”

Să considerăm următoarea secvență din şirul numeric al lui Fibonacci: 1, 2, 3, 5, 8, 13, 21, 34, 55 şi să extragem din strofa de mai sus, literele ale căror numere de ordine coincid cu termenii secvenței fibonaciene. Obținem literele:

S	O	M	O	A	S	L	U	N
19	15	13	15	1	19	12	21	14

pentru fiecare dintre ele, am scris şi rangul pe care-l au în alfabetul normal ordonat. Suma acestor ranguri este egală cu 129, şi ea nu se schimbă dacă cel mai mic rang, adică „1” rangul literei A, se scade din el şi în acelaşi timp se adună la următorul rang ca ordin de mărime, care este 12, rangul literei L.

Astfel şirul de ranguri de mai sus devine:

19 15 13 15 0 19 13 21 14

Din primele patru numere reținem numai cifrele unităților, ultimele patru numere le lăsăm neschimbate, după care toate numerele se înlocuiesc cu literele, care au aceste numere drept ranguri în alfabet adică,

9	5	3	5	19	13	21	14
I	E	C	E	S	M	U	N

secvența finală, I E C E S M U N, prin anagramare conduce la numele EMINESCU.

Este puțin probabil ca poetul să se fi gândit la această metodă de a-şi disimula numele în această poezie.

Dar să continuăm seria exemplelor.

Să presupunem următorul înscris:

„Bine că există o hotărâre a forului de judecată. Pentru mai multe noutăți, am promisiunea unui reporter care tratează cu un avocat."

Apa trece pietrele rămân."

Dacă excludem proverbul din final, prima parte a înscrisuluiare, printre altele, următoarele caracteristici statistice:

Având 107 litere şi 22 de cuvinte, rezultă o lungime medie de 4.86 litere/cuvânt, valoare identică cu aceea caracteristică limbii române.

Cele mai frecvente litere inițiale de cuvinte, din text, sunt următoarele: A, C, P, U, M, iar în limba română ordinea este S, C, P, A, I.
Mai mult, în text, nu apar ca inițiale de cuvinte, literele, S şi I, deci din acest punct de vedere, textul prezintă abateri semnificative.

Pentru frecvențele procentuale ale literelor care apar în text, avem următoarele valori:

litere	A	I	E	R	T	N
fr. în limbă	13.80	12.56	11.79	7.89	7.42	6.16
fr. În text	15.88	7.47	11.21	9.34	10.28	5.60

După cum se observă, diferențele sunt majore.

Deci, sau prima parte a înscrisului conține informația confidențială şi proverbul reprezintă cheia după care s-a făcut disimularea, sau invers, încercările făcându-se în ambele variante.

Să extragem literele inițiale ale cuvintelor de ranguri pare, din prima parte a înscrisului. Obținem secvența: B E H F J M N P R T U, din care, înlocuind fiecare literă cu rangul ei din alfabet, rezultă următorul şir numeric: 2, 5, 8, 6, 10, 13, 14, 16, 18, 20, 21.

În proverb, ultimul cuvânt îl scriem pe primul loc, după care numerotăm şirul de litere obținut adică:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
R	A	M	A	N	A	P	A	T	R	E	C	E	P	I	E	T	R	E	L	E

Din această structură extragem literele ale căror numere de ordine coincid cu termenii şirului numeric determinat anterior, literele extrase formează inforrmația căutată: **„ANA ARE PERLE”.**

Exemplul următor arată că, rezultatul obținut din analiza unui astfel de înscris, trebuie trata cu mare atenție.

Să presupunem următorul înscris:

„La anul vor supune o lege pentru exploatarea cărbunelui din partea estică a statului. Cred că voi stabili şi eu un program de viitor pentru asigurarea şi stabilizarea strict oficială a muncitorilor noştrii agricoli care vin aici. Statutul actual îi pune alături de cei puțin agreați, astfel că şi plata lor este necorespunzătoare. Atragerea lor masivă aduce statului mari venituri.”

Trecem direct la aflarea soluției.

Din toate cuvintele de ranguri pare din text, extragem a doua lor literă şi obținem informația: **„NU EXISTĂ TURIST FUGIT ILEGAL. STATE”**

Dar destinatarul, care cunoaşte convențiile stabilite şi ştie la ce onformații să se aştepte, continuă analiza soluției de mai sus.

Din acest text extrage literele care ocupă rangurile, 3, 6, 9, 12, 15, ..., şi obține informația la care se aştepta: **„EŞTI FILAT”.**

Dar să facem din nou o pauză, şi să ne punemla încercare spiritul de observație, rezolvând următoarele exerciții:

1). Cum se poate obține cuvântul DUMNEZEU, chiar şi în altă limbă dec-t româna, din următorul text:

„Descoperirea omidei, timorează”

2). Cum se obține cuvântul ABAC din bigrama LM?

Soluții:

1). Din fiecare cuvânt extragem prima şi a patra literă, rezultând secvența, D C O D T O pe care o partajăm astfel; DC O DT O care, conform substituției cifrelor prin numere în limba română, se transformă în secvența numerică, 25 8 23 8. Înlocuind aceste numere cu literele din alfabet, care au aceste numere drept ranguri, rezultă secvența YHWH, care este cuvântul DUMNEZEU scris în ebraică.

2). Soluția este imediată. Înlocuim literele din bigramă cu rangurile lor din alfabet, rezultând numărul, 1213 şi acum înlocuim fiecare cifră a acestui număr cu litera care, în alfabet are acel număr drept rang şi rezultă cuvântul, ABAC.

Revenind la exercițiile de disimulare, propunem următorul exercițiu, având textul care urmează:

„Am cumpărat din oraşi ziarele. Este plăcut de inventariat ideile noi. Gogoriţele le spun numai invidioşilor.

Apropo, l-ai citit pe Mark Twain?”

Cheia de disimulare este formată de numele scriitorului merican. Înlocuim literele lui cu rangurile lor din alfabet şi obținem şirul: 1 3 1 1 8 1 1 2 0 2 3 1 9 1 4. din care, conform convenției se elimină numerele, 8, 9 şi 0, rezultând secvența, 1 3 1 1 1 1 2 2 3 1 1 4. Numerele secvenței dacă este necesar, după care din fiecare cuvânt extragem litera care ocupă rangul identic cu numărul înscris deasupra cuvântului respectiv. Literele extrase formează expresia: **„AM DOZELE. VINO LUNI”.**

Presupunem că B aşteaptă de la prietenul A, unele date privind o anumită persoană, primind în acest sens următoarea scrisoare:

„Sunt la Uniune hotărât să urgentez afacerea şi construcția, trebuie doar semnătura. Peste ceva timp, mă voi deplasa printre cei câțiva prieteni, pentru susținerea avansurilor şi titlurilor. Dacă pot, trimit hotărârea conducerii unui inginer, având şanse pentru câştigarea concursului.”

Textul se împarte în grupe de câte trei cuvinte consecutive, şi în fiecare grupă, litera inițială a celui de-al treilea cuvânt, prin numărul pe care-l substituie în limba română, arată a câta literă din primul cuvânt se extrage. Astfel, prima grupă este formată din cuvintele: **„Sunt la Uniune”,** prima literă al celui de-al treilea cuvânt este U, care substituie numărul „1”, deci din primul cuvânt extragem prima literă, adică pe S.

Literele extrase formează expresia: **„SHE IS A TEACHER”,** dezvăluind profesia persoanei de interes.

Cu tot conținutul economic al înscrisului, el ascunde numele unui savant român de renume, pe care urmează să-l găsim:

„Nimic nu supără colaboratorii decât rudele acelora care spun prietenilor toate opțiunile colaborării, cu adnotări programatice despre sponsori.”

Textul se împarte în grupe de câte trei cuvinte consecutive şi în fiecare grupă, literele de rangul doi şi trei – în această ordine – din ultimul cuvânt prin numerele pe care le substituie, arată rangurile de pe care se reţin literele din primul cuvânt al grupei. Astfel, prima grupă este formată din cuvintele: **„Nimic nu supără”,** în care literele de rangul doi şi trei din ultimul cuvânt sunt, U care-l substituie pe „1” şi P, care-l substituie pe „4”, deci din primul cuvânt extragem prima şi a patra literă, adică pe N şi I. Continuând procesul, literele extrase conduc la numele savantului, NICOLAE IORGA.

Să reținem procedeul de disimulare folosit.

O îmbunătățire a procedeului anterior este prezentată în exercițiul bazat pe următorul text:

„Privitor la nuntă, naşii vor numai invitați din rândul celor care nu folosesc evenimentul în favoarea unor relații. Stabilirea listei nominale va fi realizată cu consultarea preotului. Dacă voi nu puteți veni, regretăm.

Vom dovedi principialitate.”

Conform convenției dintre corespondenți, din ultimul cuvânt al înscrisului se reţin numai literele distincte, în ordinea în care apar în cuvânt, litere care se numerotează, adică

P	R	I	N	C	A	L	T	E
1	2	3	4	5	6	7	8	9

obținând astfel o substituție a numerelor; 1 prin P; 2 prin R etc.

Textul se împarte în grupe a câte trei cuvinte consecutive, se reține litera inițială a celui de-al treilea cuvânt care, conform substituției de mai sus se înlocuieşte cu un număr, acest număr arată a câta literă din primul cuvânt se extrage.

Astfel, prina grupă este, **„Privitor la nuntă”,** al treilea cuvânt începe cu N, care conform substituției de mai sus, reprezintă numărul 4, deci din primul cuvânt extragem a patra literă, adică litera V.

Literele astfel extrase formează expresia **„VINO LA BACĂU”.**

În următorul text este disimulat numele EMINESCU:

„E umilit pentru că este mai posac şi nu se prea acomodează cu acei ce nu ştiu nimic”, iar în textul care urmează, numele VERONICA,

„În cazul acesta intervine profesorul numai dacă este obligatoriu ca elevii internați să răspundă pentru faptele din şcoală sau din afara ei. În celălalte situații Direcțiile de învățământ se vor sesiza din oficiu, anulând vizitele.”

În ambele cazuri disimularea s-a făcut după aceeaşi regulă, pe care urmează să o stabiliți.

Informațiile suplimentare oferite, facilitează rezolvarea.

Din primul text, începând cu prima literă, se observă următoarea secvență, E (1) M (2) I (3) N (5) E (8) S (13) C (21) U, în care numerele din paranteze desemnează numărul de litere din text, care se găsesc între literele secvenței. A rezultat deci numele EMINESCU, pe baza secvenței fibonaciene, 1, 2, 3, 5, 8, 13, 21.

În al doilea text, începând cu al doilea cuvânt, numerotăm cuvintele:

1 2 3 4 5 6 ...

Cazul acesta intervine profesorul numai dacă ...

după care, din cuvintele ale căror numere de ordine formează secvența fibonaciană de mai sus, 1, 2, 3, 5, 8, 13, 21, 34, extragem prima lor literă şi obținem secvența, CAINOREV, care citită de la dreapta, după inversarea primei bigrame, rezultă numele, VERONICA.

Să se găsească informația disimulată în următorul text:

„Respingând hotărârea plenarei, se propune acestui onorabil politician, parodiat, să accepte constatările presei că romantismul este ceva dăunător. Responsabilitatea contează."

Conform convenției, parola este formată din penultimul cuvânt al textului, din care se rețin literele distincte, care se numerotează,

R E S P O N A B I L T

1 2 3 4 5 6 7 8 9 10 11

obținând astfel o substituție a numerelor.

Textul se împarte în grupe de câte trei cuvinte consecutive, primele două litere din primul cuvânt al grupei se transformă în numere conform substituției de mai sus, iar aceste numere arată care litere din al treilea cuvânt al grupei se vor reține.

Astfel, prima grupă este formată din cuvintele, **„Respingând hotărârea plenarei"**, primul cuvânt are primele două litere, R şi E, care, conform substituției, conduc la numerele, 1 şi 2, deci din al treilea cuvânt al grupei, reținem prima şi a doua literă, adică, PL etc. Literele astfel reținute formează expresia**: „PLEC DIN ȚARĂ".**

Pentru cei familiarizați cu jocurile rebusiste, este uşor să observe legătura dintre „scrierile disimulate", ca gen criptologie şi acrostihul, ca gen rebusistic.

Următorul exemplu este semnificativ în acest sens.

Se cunoaşte faptul că G. Coşbuc (1866-1918) a folosit anagrama pentru a-şi semn aunele poezii. Astfel, poeziile: „Unde zbor”, „Filozofii şi plugarii”, „Aş vrea să fiu”, „Două întrebări” şi „Inima mamei” au fost semnate C. BOŞCU, care este o anagramă a numelui său.

Cercetând şi alte poezii, înclinăm să credem că poetul a folosit şi acrostihul, uneori mai estompat, de tipul acelora folosit şi de Eminescu.

În acest sens vom considera ultima strofă din poezia lui Coşbuc „Fata morarului”,

„O macină grâul mai bine
Şi-nvârtăte, roată, mereu!
Că lumea se-nvârte cu mine
Şi vreu, şi eu nu ştiu ce vreu!
Ba lasă, că ştiu eu ce vreu:
Aş vrea să fiu, roată, supt tine”

Extragem literele inițiale ale versurilor, adică, OSCSB, ultima bigramă inversată o scriem pe primul loc şi obținem, ABOSCS. Înlocuim aceste litere cu rangurile lor din alfabet, apoi la această secvență numerică îi adunăm „cheia” simetrică, (2 0 0 0 0 2) după care numerele obținute se înlocuiesc cu literele care, în alfabet, au aceste numere drept ranguri. Deci

A	B	O	S	C	S
1	2	15	19	3	19
2	0	0	0	0	2
3	2	15	19	3	21
C	B	O	S	C	U

A rezultat, C. BOŞCU, semnătura folosită de poet.

Referitor la aceste modalități de comunicare, amintim de acțiunile întreprinse de autoritățile americane, începând cu anul 1940, pentru controlul tuturor canalelor de comunicații care puteau fi folosite de serviciile de spionaj străine care operau pe teritoriul american.

În acest sens ei au înființat un puternic serviciu de cenzură, la Hotelul Princess Hotel din Insulele Bermude, unde se deschideau şi analizau toate scrisorile primite sau expediate din America, interceptau convorbirile telefonice, analizau careurile de cuvinte încrucişate, scrisorile în cadrul concursurilor de şah prin corespondență etc.

Analiza scisorilor care puteau conține şi comunicări disimulate, ridicau probleme deosebite. O problemă cu care se putea confrunta, este semnificativă în următorul text:

„**Toată această criză este privită cu mare îngrijorare. Miile de intelectuali care există îşi abandonează munca. Statul este neputincios în situația de criză. Numerele de telefon cerute sunt, 2765033 şi 2713149.”**

Aflarea informației disimulate este dificilă, dar cu efort, răbdare şi spirit de observație, se ajunge la soluție.

Astfel, toate cuvintele de ranguri impare, din text, se împart în grupe a câte trei cuvinte consecutive, şi în fiecare grupă, din primul cuvânt se reține prima literă, din al doilea a doua literă, iar din al treilea cuvânt se reține a treia literă, după care procedeul se repetă. Prima grupă este formată din cuvintele: „**Toată, criza, privită”** şi conform convenției, se reţin literele, TRI. Continuând procedeul, rezultă informația **„TRIMITE BANII”.**

Dar, intrigat de cele două numere de telefon, respectivul cenzor continuă analiza, ajungând la următoarea constatare:

Fiecare număr de telefon are şapte cifre, atunci din text reține primele 14 litere, pe care le numerotează de la 1 la 7, repetând evident această secvență numerică, adică

1	2	3	4	5	6	7		1	2	3	4	5	6	7
T	O	A	T	Ă	A	C		E	A	S	T	Ă	C	R

Din al doilea număr de telefon consideră primele trei cifre, adică 2, 7, 1 şi din a doua secvență de mai sus, reține literele corespunzătoare lor, adică, ARE, apoi consideră primele trei cifre din primul număr, adică, 2, 7, 6 şi reține literele corespunzătoare lor, din prima secvență, adică, OCA. Repetă procedeul, considerând următoarele trei cifre din al doilea număr, adică, 3, 1, 4 şi literele corespunzătoare din a doua secvență, adică, S, E, T, trecând la primul număr de telefon, din care este nevoie numai de a patra cifră, adică 5 şi litera corespunzătoare ei din prima secvență, adică Ă.

Literele astfel extrase formează textul, **„ARE O CASETĂ”.**

A obținut astfel, pe baze logice, două informații fără a dispune de criterii pentru a decide care este informația adevărată.

Se presupune că, atunci când cenzorii se confruntau cu astfel de situații, modificau unelel cuvinte din text, sau numerele care apăreau, astfel încât nici corespondenții nu se înțelegeau între ei, fiind obligați să-şi ceară explicații şi astfel se desconspirau.

Următorul exemplu arată că, problema alegerii informației reale care a fost disimulată, poate fi şi mai dificilă.

Presupunem următorul text:

„Nu ştiu cum vor vota, ei sunt noi între voi: Dacă o mai consideri o posibilitate deosebită, să eviți ultranaționaliştii, e obligatoriu. Sună-mă: 4635214”.

Din textul aflat până la cele două puncte, formăm structura: N (4) U (6) V (3) E (5) N (2) I (1) T (4) I, în care numere din paranteze, care sunt chiar cifrele numărului de telefon, reprezintă numărul de litere din text, care separă literele din structură, litere care formează expresia, **„NU VENIȚI”.**

Dacă notăm lungimea în litere a textului care urmează după cele două puncte – este vorba de lungimea în litere a cuvintelor din acest text – obținem un şir numeric, şi dacă înlocuim fiecare număr cu litera care, în alfabet are acest număr drept rang, rezultă

4	1	3	9	1	12	9	2	5	18	1
D	A	C	I	A	L	I	B	E	R	A

deci informația **„Dacia liberă”.**

Să considerăm primele 6 litere ale textului care urmează după cele două puncte, litere pe care le numerotăm adică,

1	2	3	4	5	6
D	A	C	Ă	O	M

iar din această corespondență, culegem literele în ordinea din numărul de telefon, rezultând expresia, **„AM COADĂ”,** deci respectivul individ a observat că este filat.

S-au obținut deci trei informații, din care trebuie aleasă informația reală.

Şi acum un test de perspicacitate:

„Cum se poate obține cuvântul ARD din expresia, LE DAM UNT”?

După mai multe încercări, se ajunge şi la a încerca soluționarea cu ajutorul Codului Morse, procedând astfel; în fiecare cuvânt din expresie, consoanele se înlocuiesc cu „PUNCT”, iar vocalele cu „LINIE”, structura obținută se descifrează cu Codul Morse.

Astfel, cuvântul LE, devine, „PUNCT – LINIE”, care în acest Cod reprezintă litera Ă.

La fel, DAM devine „PUNCT – LINIE – PUNCT”, adică R, iar UNT devine „LINIE – PUNCT – PUNCT”, adică litera D.

Aflând informația disimulată în textul care urmează, veți găsi numele unei matematiciene engleze, care a introdus pentru prima dată „cartelele perforate” în domeniul calculatoarelor. Dar iată textul: „**Am vizitat oraşele: Arad, Alba, Nădlac. Emil e grozav de vesel, nu face curte, e păcat”.**

La o analiză atentă se observă că, în textul care urmează după cele două puncte, tot a şaptea literă este o consoană, deci pentru analist acest fapt reprezintă un semnal.

Se scrie acest text pe coloane, fiecare conținând câte şapte litere, şi din acest tabel considerăm prima şi a patra linie, adică

A	A	E	O	E	A	E
D	D	L	V	L	C	A

citind aceste litere pe coloane, de sus în jos, obținem numele căutat, ADA de LOVELACE, contesă, fiica lui Byron, care a aplicat la maşina de calcul a matematicianului englez Babbage, tehnica francezului Jacquard, de control automat al războaielor de țesut prin „cartele perforate”, transformând maşina de calcul în primul calculator.

Următorul exemplu aduce în scenă puțină matematică.

Să considerăm următorul text, în care se găseşte disimulată o anumită informație, pe care trebuie s-o aflăm:

„Statistica reuşeşte, uneori rezolvări spectaculoase. M-am orientat spre numerele remarcabile, inconfundabilul PI, împreună cu

„ingeniosul" număr recunoscut de aur. Am tratat astfel multe opere, ajungând să confirm, prin fapte, contribuția generală a matematicii."

Considerăm rezolvarea destul de dificilă, dar referirile la cele două numere remarcabile, ajută analiza şi soluționarea problemei.

Primul număr care apare este PI (raportul dintre lungimea cercului şi diametrul său), având valoarea cu trei zecimale egală cu 3,141 iar al doilea număr este „celebrul număr de aur", având valoarea cu trei zecimale egală cu 1,618.

Cu aceste două numere (eliminând virgula) formăm un şir numeric, considerând alternativ numărul PI urmat de „numărul de aur", deci 3141161831411618 ....

Acest şir numeric se scrie, cifră cu cifră, deasupra tuturor cuvintelor de ranguri impare din text, şi din fiecare cuvânt se extrage litera care ocupă în el, rangul egal cu numărul înscris deasupra cuvântului respectiv.

Literele astfel extrase conduc la informația, **„AU CONFISCAT MARFA".**

Cele prezentate anterior, ne sugerează următorul exercițiu, potrivit pentru testarea intuiției şi a spiritului de observație, şi anume: se dă un text oarecare şi se cere ca, într-un interval de timp să se găsească cât mai multe cuvinte, sau expresii, care sunt „disimulate" în text, pe baza unor secvențe fibonaciene.

Reamintim că, o secvență numerică se numeşte fibonaciană, dacă fiecare termen al ei, începând cu al treilea, este egal cu suma celor doi termeni precedenți. Exemple de astfel de secvențe; 1, 2, 3, 5, 8; 2, 7, 9, 16, 25 etc.

Pentru a lămuri pe deplin lucrurile, să considerăm următorul text: **„CA O MAMĂ ŞTIU SĂ-L IERT".**

Iată câteva cuvinte, sau expresii, deduse din el, pe baza unor secvențe fibonaciene:

- începând cu a doua literă a textului, avem următoarea structură; a (1) m (2) a (3) u (5) r, unde numerele din paranteze formează secvența fibonacianâ, 1, 2, 3, 5 şi reprezintă numărul de litere din text, care separă literele din structură. Rezultă din structură expresia, **„am aur”,**

- dacă parcurgem textul în sens invers, începând cu ultima literă, avem structura, t (1) e (1) l (2) u (3) ă, cu semnificațiile de mai sus, ne conduce la expresia, **„te luă”** etc.

Ca exercițiu mai complex, propunem drept text strofa a şaptea din poezia eminesciană, **„Floare albastră”:**

„Şi mi-i spune – atunci poveşti
Şi minciuni cu a ta guriță,
Eu pe-un fir de romaniță
Voi cerca de mă iubeşti.”

Din care vom prezenta numai 2-3 cuvinte care se obțin:

- începând cu prima literă a cuv-ntului „spune”, din primul vers, avem structura, s (5) t (5) o (10) e, în care secvența fibonacianâ, 5, 5, 10, conduce la cuvântul „stoc”,

- începând cu a 12-a literă, din primul vers, apare structura, T (7) E (8) C (15) E (23) R, secvența fibonacianâ, 7, 8, 15, 23 conducând la secvența „TECER” din care rezultă expresia, „TE CER”.

Să notăm rangurile din alfabet ale acestor litere, 20 . 5 . 3 . 5 . 18 şi să adunăm numerele vecine, adică 20+5=25; 5+3=8; 3+5=8; 5+18=23, obținem secvența, 25 8 8 23 pe care o scriem astfel, 25 8 23 8 şi apoi înlocuim fiecare

număr cu litera din alfabet, care are acel număr drept rang, adică, Y H W H, secvență care reprezintă cuvântul Dumnezeu, scris în ebraică.

- dacă vom considera ultima literă a strofei şi trecem la primul vers, avem structura, I (2) M (3) P (5) U (8) T (13) A (21) M şi deci secvența fibonaciană, 2, 3, 5, 8, 13, 21, ne-a condus la cuvântul, IMPUTĂM etc.

Să revenim însă la problematica noastră, printr-un nou exemplu:

Considerăm următorul text, trimis cetățeanului B, aflat în cercetări: **„Cronica mea, documentară, va incrimina controlul şi procurorul care anchetează cazul. Atitudinea lor pregăteşte condamnarea, opunându-se vehement actelor din dosarele în lucru. Pentru început contestăm problematica din citație, adresându-ne parchetului."**

Rezolvarea este dificilă, dar perseverența şi intuiția vor învinge.

Cheia problemei este formată din primele două litere ale primului cuvânt din text, adică „CR". Se scriu rangurile lor din alfabet rezultând secvența, 318 după care numerele vecine se adună, din rezultatele adunărilor, atunci când apar, se elimină numărul nouă şi zero. Deci avem, 3+1=4, care se scrie după 8 din secvență, apoi 1+8=9 care nu se scrie, secvența a devenit, 3184, urmează, 8+4=12, secvența devine, 318412, apoi 4+1=5 şi 1+2=3, secvența a devenit, 31841253 ... şi se continuă din aproape în aproape prin adunarea în „lanț" a numerelor alăturate. Primii 15 termeni ai şirului astfel construit, sunt: 3 1 8 4 1 2 5 3 7 8 1 1 5 2 6. Acest şir se scrie, termen cu termen, deasupra cuvintelor de ranguri pare din text, şi din fiecare cuvânt se extrage litera care, în cuvânt, are rangul egal cu numărul înscris deasupra cuvântului respectiv.

Literele extrase conduc la mesajul, „AVOCAT AUREL ILIE", deci numele acestuia prezenta interes pentru cetățeanul B.

Următorul exemplu este mai simplu de rezolvat.

Să considerăm următorul text:

„Am realizat că dorința ta de reevaluare favorabilă a terenului te-a solicitat mult, în faza de reanalizare a faptelor. Mi-e nu-mi surâde donația, situația fiind fără viitor. Soluția, după refundamentare se doreşte a fi realistă, dar ministerul a scăpat situția de sub control, propunând doar bazaconii."

După o analiză atentă a textului, se ajunge şi la următoarea constatare; numărul mare, aproximativ 41,30 la sută, al cuvintelor care încep cu una dintre denumirile notelor muzicale: DO, RE, MI, FA, SOL, LA, SI, şi de aici soluția este aproape. Din toate aceste cuvinte se reține litera care urmează după denumirea notei muzicale. Astfel, din cuv-ntl „REALIZAT", se reține litera A, din cuvântul „SOLICITAT" se reține litera I etc.

Literele astfel reținute formează informația care a fost ascunsă: **„ARE VIZĂ PENTRU FRANȚA".**

Mergând oarecum, pe varianta de mai sus, din analiza următorului text, să se afle titlul unei poezii a lui G. Bacovia;

„La casa din Sighişoara trebuie să fac studii de fesabilitate pentru a realiza asfaltarea la curtea interioară. Singurul scop este să reduc gardul viu din fața clădirii".

Din primul cuvânt care urmează unui cuvânt care începe cu denumirea unei note muzicale, se reține a doua sa literă. Literele astfel reținute conduc la titlul poeziei: **„LACUSTRA".**

Încercați-vă forțele găsind adevăratul mesaj ascuns în următorul text:

„Armatele puternice colaborează decizional, stimulând dotarea conducerii tactice stabilite după zona patrulară, încredințată unui comandant".

Textul se împarte în grupe de câte două cuvinte consecutive, al doilea cuvânt din fiecare grupă are prima şi a treia literă, numai litere care substituie numerele şi ele arată care litere din primul cuvânt al grupei vor fi reținute. Astfel, prima grupă este formată din cuvintele, **„Armatele puternice”**, al doilea cuvânt având prima literă P=4 şi a treia T=3, deci din primul cuvânt extragem a patra literă care este A şi a treia, care este M, ş.a.m.d.

Literele astfel extrase conduc la mesajul **„AM OBȚINUT BANII”.**

Următorul exercițiu este asemănător cu acela cu care am început acest material, referitor la modalitățile de transmitere folosite de Paul Rosbaud.

La articolul având următorul început:

„Anatole France (1844-1924). Poète, romancier, Journaliste et critique, Anatole France (pseudonime d’Anatole Thibault) débute en littérature par des vers parnassiens ...”, Rosbaud adaugă, în calitate de redactor, următoarea NOTĂ a redacției: **„A fost onorat prin conferirea premiului Nobel pentru toată opera. Este mândria țării sale, a întregii Europe, a lumii întregi. Literatura, prin acest reprezentant, face pasul temeinic către apropierea tuturor națiunilor.”**

Ştiind că Anatole France este ... cheia problemei, găsiți informația transmisă de P. Rosbaud.

Scriem literele distincte din numele scriitorului şi le numerotăm, adică:

A N T O L E F R C
1 2 3 4 5 6 7 8 9

obținând o substituție a literelor respective.

Extragem literele inițiale ale cuvintelor de ranguri impare din textul care urmează după expresia NOTĂ A REDACȚIEI, obținând secvența, AOCNTETAELLAFTAN, care, conform substituției de mai sus,conduce la şirul numeric: 1492363165517312, care se înscrie, termen cu termen, deasupra tuturor cuvintelor din textul în limba franceză şi din fiecare cuvânt extragem litera indicată de numărul înscris deasupra cuvântului respectiv.

Literele extrase formează mesajul: **„PASTILA POATE ARDE”**.

Şi acum un exercițiu foarte simplu.

Denumirea resursei strategice a epocii informative este înserată în următorul text:

„În două zile începem oficial construcția promisă, un magazin al tinerilor ingineri angajați.”

Soluția este aproape imediată. Numeralele din text arată care sunt literele care se extrag. După DOUĂ, din toate cuvintele extragem literele de locul al doilea, deci INFOR. După UN, extragem inițialele cuvintelor care urmează, deci MATIA. Alăturând cele două secvențe obținem denumirea căutată: **INFORMAȚIA.**

Continuăm seria exemplelor noastre, cu următorul text care ascunde o informație pe care trebuie să o găsim.

„Marți am avut o demonstrație la o facultate de la Academia Comercială, mi-au recunoscut titlul putând cumula astfel orele. Titularul catedrei a formulat unele propuneri, optând pentru comasarea studenților din alte institute. Poate vor aduce noi cadre, evident titulari şi invitați, pentru creşterea interesului tinerilor din zonă, care frecventează Academia.”

Exercițiul este destul de dificil, dar prin perseverență şi intuiție se ajunge la soluție.

Cheia este cuvântul MARȚI, din care, scriind rangurile din alfabet ale acestor litere, se obține succesiunea, 13118209, din care eliminând pe zero şi nouă, rezultă secvența numerică, 131182. Cifră cu cifră scriem această secvență deasupra cuvintelor care, în text, au rangurile 2, 5, 8, 11, 14, 17, ..., adică din trei în trei, secvența numerică repetându-se de câte ori este necesar, şi din fiecare cuvânt extragem litera care, în cadrul lui, ocupă rangul identic cu numărul înscris deasupra cuvântului.

Literele astfel extrase formează informația căutată şi anume: **„AM FĂCUT ROST DE VIZĂ”.**

Un exercițiu la fel de dificil este următorul, legat de un presupus anunț dintr-un ziar, având următorul conținut:

„Vând ieftin teren pentru grădină, sau construcție, apropiere localitate, plata numai în dolari.

Opțional pot executa îndepărtarea buruienilor, operațiunea costă puțin. Construcția poate fi începută în două luni, după virarea sumelor, familiei proprietară.”

Conform convenției dintre corespondenți, pentru aflarea informației, se procedează astfel:

Din al doilea paragraf se extrag literele inițiale ale cuvintelor de ranguri impare adică, OEBCCFILVF după care fiecare literă se înlocuieşte cu rangul ei din alfabet, rezultând următoarea secvență numerică: 1 5 5 2 33 6 9 1 2 2 2 6, care se scrie, cifră cu cifră, deasupra tuturor cuvintelor din primul paragraf al anunțului, urmând ca din fiecare cuvânt să reținem litera care ocupă locul egal cu numărul scris deasupra cuvântului respectiv.

Literele extrase formează textul: **„VINE AUREL LUNI”.**

Referitor la acest exemplu, se pare că metoda de a transmite mesaje conținând comunicări disimulate, prin enunțuri în ziare, a fost folosită în cel de-al doilea război mondial.

Astfel, Paul Thűmmel, celebrul informator „A-54” al serviciului ceh de informații, lucrător în serviciile germane de informații încă din 1928, a folosit această modalitate.

Aflat la Praga, pentru a-şi contacta ofițerul de legătură, a dat în „Norodni Politika” din 17 martie 1940, următorul anunț:
„Frantişek, totul e în regulă, te ține minte şi te caută Perticka”, din care ofițerul a dedus data şi locul de întâlnire.

Prin câteva exemple anterioare, am sugerat faptul că, studierea scrierilor disimulate poate fi utilă şi pentru analiza unor texte poetice sau documente vechi de interes. Prezentăm în continuare un rezultat obținut din analiza unui astfel de document mai puțin cunoscut.

Este vorba de textul interogatoriului luat lui Eminescu, în stabilimentul din strada Plantelor, la 12 iunie 1889. descifrarea acestui document, am prezentat-o în articolul **„Un document şi ... enigmele lui”** publicat în revista SAECULUM, Focşani, an. II, nr. 5 – iulie 2003.

Dar să vedem câteva constatări rezultate şi care au legătură cu scrierile disimulate.

Întrebarea a doua din interogatoriu este următoarea, **„Pentru ce?”,** iar răspunsul, presupus a fi dat de Eminescu, a fost: **„Pentru că eu fiind moştenitorul lui Matei Basarab, regele se temea să nu-i iau moştenirea”.**

Întrebarea conține 8 litere, din textul răspunsului extragem a 16-a, a 24-a; a 32-a; a 40-a şi a 48-a literă, deci din opt în opt, câte litere are

întrebarea, pe care o putem considera cheia de disimulare. În ordinea extragerii lor, aceste litere formează cuvântul, MOARE. Coincidență sinistră, căci, la trei zile după interogatoriu, Eminescu a murit.

Răspunsul la întrebarea a patra din interogatoriu începe cu expresia **„Un om bogat care are”**, urmată de numărul 48 şi un text care pentru demersul acesta, nu prezintă interes.

Numărul 48 are ca divizori numerele, 1, 2, 3, 4, 6, 8, 12, 16 şi 24.

Din expresia cu care începe acest răspuns, extragem literele care ocupă pozițiile 4, 6, 8, 12, 16, începând deci cu a patra literă, fiind vorba de al patrulea răspuns, restul numerelor sunt divizorii lui 48. literele astfel extrase formează cuvântul, MOARE, care vine parcă să confirme rezultatul anterior.

Dar să revenim la problemele noastre, supunând atenției următorul text, din care trebuie să găsim informația care a fost ascunsă:

„**Având o problemă mai încurcată, trebuie întrebat un expert, care să ştie interpreta toate prevederile legale, întrucât intervenția controlului poate dispune uşor anularea contractului. Nu poți şti cine intreprinde acest control.”**

Aştept cu nerăbdare să ne revedem.”

Cheia de disimulare este dată de ultima expresie a textului, în care, pentru fiecare cuvânt, notăm rangurile ocupate de consoane, rezultând următoarea secvență numerică: 2, 3, 5, 6, 1, 1, 3, 5, 6, 8, 1, 1, 1, 3, 5, 7, pe care o scriem, număr cu număr, deasupra cuvintelor de ranguri impare din text, urmând ca, din fiecare cuvând să extragem litera care, în cuvânt, ocupă locul identic cu numărul scris deasupra cuvântului respectiv. Literele astfel

extrase formează informația căutată şi anume: **„VORBEŞTE CU DANIEL.”**

Şi acum un exercițiu mai simplu pentru relaxare.

Să considerăm următorul text, schimbat în preajma unor examene, evident ipotetic:

„La vară vizităm celebrele construcții orădene, studiind vestita arhitectură. Plecarea este planificată, prețurile achitate, controlul actelor făcut. Primele contacte directe, au finalizat atent cuprinsul vizitei.”

Pentru aflarea informației care a fost ascunsă, procedăm astfel: împărțim textul în grupe de câte 5 cuvinte consecutive şi, în fiecare grupă, din primul cuvânt extragem prima literă, din al doilea cuvânt a doua literă, ..., din al cincilea, a cincea lui literă şi se obțin secvențele: LAZET, OTSIA, ELEIR, AAITC, respectiv, AIERT.

Scriem toate aceste secvențe de la dreapta la stânga şi le alăturăm, obținem informația: „TEZA LA ISTORIE, LECȚIA A TREIA”. Se mai întâmplă în învățământul de astăzi astfel de lucruri.

Exercițiul care urmează, dispunând de informații suplimentare, s-ar putea să nu ridice probleme deosebite pentru rezolvare.

În textul care urmează este disimulat numele unui remarcabil om de ştiință român:

„Un pion cu sticlă este pregătit de un cursant, pentru unele dintre companiile din Bucureşti care au profituri.”

Cheia de disimulare se poate afla dinanaliza următorului text: „**Face pe mahmurul având apucături deranjante, râde de specialişti.”**

Dacă ați aflat cheia corectă, aplicați-o următorului text, pentru a afla denumirea recompensei meritată de acest savant român, textu este: **„Sunt o babă veselă, dar cultă”.**

Începem rezolvarea de la ultimul text, gândindu-ne la diferite recompense meritate: „statuie” şi „academician” nu pot fi acceptate deoarece în text nu apare litera „I”. Dar, dacă nu este matematician, atunci recompensa supremă este PREMIUL NOBEL.

Formăm, cu literele textului, cuvântul NOBEL, observând că acest lucru este posibil dacă extragem literele cu numerele de ordine, 3, 5, 8, 13, 21, această secvență numerică este o secvență fibonaciană (fiecare termen, începând cu al treilea, este egal cu suma celor doi termeni precedenți). Dacă aceasta este cheia, mergem la primul text şi extragem literele cu numerele de ordine, 3, 5, 8, 13, 21, 34, 55, 89 obținând numele savantului, PAULESCU, descoperitorul insulinei, deci cheia a fost confirmată.

În lipsa celui de-al treilea text, trebuia să găsim cheia din cel de-al doilea text. Analizând acest text, ajungem şi la următoarea constatare:

Numerotăm literele cuvintelor şi înlocuim apoi literele cu rangurile lor din alfabet:

1 2 3 4	1 2	1 2 3 4 5 6 7 8 ....
F A C E	P E	M A H M U R U L ....
6 1 3 5	16 5	13 1 8 13 21 18 21 12

Se observă că, în primul cuvânt, literele de pe locurile 3 şi 4, au rangurile din alfabet, 3 şi respectiv 5. În cuvântul al treilea, literele tot de pe locurile 3 şi 4, au rangurile din alfabet, 8 respectiv 13. Cele patru ranguri reținute formează secvența, 3, 5, 8, 13. Continuând procedeul se ajunge la concluzia că, din cuvintele de ranguri impare se extrag literele de pe locurile

3 şi 4 şi se substituie cu rangurile lor din alfabet, obținându-se cheia, adică secvența fibonaciană, 3, 5, 8, 13, 21, 34, ...

Pentru următorul exercițiu nu vom da nici o informație suplimentară.

Textul de analizat este:

„Un bătrân a şutit, în veselie, locuința la Sinaia.

Cafeaua face inoportună operația, bea dimineața ceai îndulcit."

Analizăm pentru început prima frază a textului (textul de la prima literă până la ultimul punct), formând cuvinte, sau expresii inteligibile în limba română, urmând ca apoi să stabilim care este adevărata informație care a fost ascunsă.

Evident că, luând la întâmplare litere din acest text, putem forma numeroase cuvinte şi expresii inteligibile, dar le vom reține numai pe acelea care au o anumită legitate de formare, sau pot fi legate eventual de al doilea paragraf al textului.

Considerăm literele acestui text numerotate, de la unu la 39, câte litere are.

Dacă considerăm literele cu numerele de ordine: 2, 4, 9, 12, 15, 16, 19, 26, 27, 29, 34, 38, obținem expresia, **„N-A ATINS CUTIA",** iar literele cu numerele de ordine: 8, 11, 17, 20, 29, 35, conduc la expresia, **„NU VENI"**.

Începând cu a 12-a literă şi parcurgând textul circular, deci după ultima sa literă, se reia textul de la început, avem structura, T (2) I (3) S (5) O (8) S (13) A, construită pe baza secvențelor fibonaciene, 2, 3, 5, 8, 13, deci o regulă. Citind de la dreapta la stânga literele din structură, obținem expresia **„A SOSIT"**, cu referire probabilă la o persoană, la o sumă de bani, la o marfă etc. În orice caz reține atenția.

Începând cu a 9-a literă, avem structura, A (3) I (6) E (9) T (15) A (23) L, construită pe baza secvenței fibonaciene, 3, 6, 9, 15, 24, aceste numere aflate în paranteze reprezintă numărul de litere din text, care separă literele din structură, litere care citite de la dreapta, conduc la **expresia „LA TEIA”**, probabil o păersoană cu care trebuie să se întâlnească, sau să-i paseze ceva etc. Reține deci atenția.

Dacă extragem literele cu numerele de ordine, 3, 6, 9, 15, 24, 39, care formează secvența fibronaciană de mai sus, obținem cuvântul **„BRĂILA”.**

Deci aceeaşi secvență ne-a condus la două informații diferite, dar demne de a fi reținute.

Căutăm atunci, în al doilea paragraf al textului, o legătură cu această secvență fibonaciană, în ipoteza că aceasta este cheia de disimulare.

Dacă din această parte extragem literele inițiale ale cuvintelor obținem succesiunea, C F I O B D C I, din care, înlocuind literele cu rangurile lor din alfabet, obținem chiar secvența fibonaciană, 3, 6, 9, 15, 24, 39, folosită mai sus şi care ne-a condus la cuv-ntul „BRĂILA”, aceasta este deci informația ascunsă. Evident că, în cazuri similare, informațiile despre corespondenți, preocupări, medii frecventate etc. ajută la aegerea adevăratei informații, deci la eliminarea acelora apărute întâmplător.

În anumite situații, informația care urmează a fi disimulată, înainte de această operațiune, este supusă unor modificări convenite, astfel încât cel care o caută găseşte această transformantă, urmând să determine respectivele transformări, pentru a ajunge la adevărata informație care a fost ascunsă.

Astfel, să presupunem că vrem să ascundem într-un text, numele poetului EMINESCU. Scriem o anagramă a numelui (anagramele erau mult practicate în epoca poetului, fie aceasta următoarea, CEISUMEN, după care

modificăm două litere, de exemplu a 4-a şi a 8-a, înlocuindu-le cu cele care le preced imediat în alfabetul normal ordonat, adică în loc de S scriem R, iar în loc de N, scriem M, anagrama devine, CEIRUMEM şi aceasta va fi secvența care va fi ascunsă.

Pentru că aceste considerații să nu pară simple speculații teoretice, prezentăm un exemplu concret.

Să considerăm titlul poeziei eminesciene, **„CARE-I AMORUL MEU ÎN ASTĂ LUME”**, numerotând literele acestui text, începând cu prima, după care, parcurgând textul circular, extragem literele ale căror numere de ordine formează secvența fibonacianã; 1, 4, 5, 9, 14, 23, 37, 60, obținând secvența, C E I R U M E N, care este chiar anagrama, modificată, prezentată mai sus.

Textul are 24 de litere, dublul acestui număr este 48, urmând ca în secvența de mai sus, să înlocuim două litere cu acelea care le urmează imediat în alfabet, numărul 48 ne spune să înlocuim liera a 4-a, deci pe R cu S, şi a 8-a, deci pe M, din final cu N, secvența devine, CEISUMEN, care este o anagramă a numelui, EMINESCU.

Următorul exemplu evidențiază o altă modalitate de disimulare relativ uşor de folosit.

Dar iată textul care trebuie analizat:

„Străinii socotesc că scopul sindicaliştilor este retragerea investitorilor cunoscuți că trişază. Sindicaliştii studiază propunerile statului, fiind reținuți pentru moment. Trimişii lor vor rupe contactele dacă nu servesc scopurilor lor. Totuşi există speranțe dacă guvernul nu respinge în bloc propunerile, reținând pentru studiu o parte din ele, salvând intreprinderea.”

Cheia problemei este dată de primele trei litere ale textului, respectiv, S, T, R folosite în felul următor; din toate cuvintele din text, începând cu al doilea, care încep cu una dintre aceste litere, se extrage a treia literă. Literele astfel extrase formează informația căutată: „CONTINUAȚI PROTESTUL”.

În următorul text este disimulat numele unui remarcabil fizician român:

„Portul tradițional reuneşte frumusețea teritoriilor noastre. Trebuie reluată practica festivalurilor, reintroducerea studierii porturilor în şcoli, teologii pot contribui la renaşterea acestor practici.

Trecutul respectat este expresia recunoaşterii geniului popular, a eliminării răului din societate.”

Ca metodă de disimulare, exercițiul este asemănător celui precedent, dar în acest caz, cheia este dată de literele de rang 3 şi 4, deci R şi T, din primul cuvânt al textului. Cuvintele din text care încep cu aceste litere, conțin pe poziția a treia literele informației. Culegând aceste litere aflăm numele fizicianului din Cluj, AUREL IONESCU (1902-1954), cel care a elaborat metoda de preparare industrială a acetilenei.

Să presupunem că, un cetățean a primit de la amicul său, la un anumit interval de timp, următoarele două înscrisuri:

Primul înscris:

„Am debutat în acest an, prelucrând din muzica populară trei cântece specifice comunității turce dobrogene. Prelucrarea se reduce la o oarecare diminuare a tratării tematice, plus eliminarea repetițiilor de care sunt sătul.”

Al doilea înscris:

„Se poate prelucra muzica populară, respectând strict tonalitățile instrumentelor. Practic nu trebuie să modifici mult tematica.

Tu unde îşi petreci concediul?”

Pornind de la ipoteza că, pentru ascunderea informațiilor s-a folosit acelaşi procedeu, înscrisurile provenind de la aceeaşi persoană, prin suprapunerea textelor şi formarea cuvintelor cu litere care ocupă în ambele texte aceleaşi ranguri, trebuie să se ajungă la soluție, evident cu efort şi atenție. Suprapunerea textelor se poate face în totalitatea lor, sau numai a cuvintelor de ranguri pare, sau a celor de ranguri impare.

Dacă se suprapun cuvintele de ranguri impare, se ajunge la descoperirea celor două informații care au fost ascunse, procedând astfel: în fiecare înscris, cuvintele de ranguri impare, se împart în grupe de câte 4 cuvinte consecutive, şi în fiecare grupă, din primul cuvânt extragem a treia literă, din al doilea prima literă, din al treilea a patra literă iar din al patrulea cuvânt extragem a cincea literă, deci cheia de extragere a literelor este, 3, 1, 4, 5.

Din primul text rezultă informația, „BĂLCESCU DOI AUREL”, probabil adresa unei întâlniri şi persoana căutată.

Din al doilea text rezultă informația, „AM PLĂTIT”, cu semnificația cunoscută de corespondenți.

Dar, expresia din finalul celui de-al doilea text, conține cheia de culegere a literelor. Astfel, literele inițiale ale celor patru cuvinte, T, U, P, C, pe baza substituției numerelor în limba română, conduc la secvența numerică, 3145, semnalată mai sus.

Exemplul care urmează ridică din nou problema stabilirii cu certitudine a adevăratei informații, disimulate într-un text.

Să considerăm următoarea comunicare:

„Voi veni singur, şi până luni organizăm o plecare alăturându-ne orădenilor. Plăteşte autobuzul achiziționat şi alege drumuri umblate din Ardeal."

Apreciem că rezolvarea nu ridică probleme deosebite.

Considerăm cuvintele de ranguri impare, constituite în grupe de câte trei cuvinte consecutive şi din fiecare grupă extragem literele după următoarea regulă; din primul cuvânt prima literă, din al doilea a doua literă, şi din al treilea cuvânt a treia literă. Literele extrase formează expresia „VINO LA ALBA".

Confuzia este astfel instalată, evident însă că nu pentru cei doi corespondenți.

Exemplul acesta subliniază din nou faptul că, la baza unor astfel de comunicări se află convențiile stabilite între corespondenți şi faptul că pentru „intrus" necunoaşterea convenției poate să-l pună în situații greu de depăşit. Nu se poate exclude nici ipoteza ca unul sau două dintre mesajele care ar putea fi deduse, să fie introduse chiar de corespondenți cu scopul de a „acoperi" mesajul adevărat.

În următorul exemplu, textul aduce informații suplimentare, care pot ajuta la obținerea soluției:

„Matematician autentic, celebru, angrenat în criptoanaliză, aduce remarcabile aplicații noutăților inginereşti. Este un specialist regretat, moare tânăr."

Cheia de disimulare folosită este formată din primul cuvânt al textului, deci cuvântul MATEMATICIAN. Înlocuim literele distincte din acest cuvânt, MATEICN, cu rangurile lor din alfabetul normal ordonat, şi din şirul numeric rezultat, eliminăm pe zero şi pe nouă, obținând cheia de disimulare, 13125314, pe care o scriem, cifră cu cifră şi repetând-o dacă este nevoie, deasupra tuturor cuvintelor textului, din fiecare cuvânt extrăgând litera care ocupă, în cadrul lui, locul identic cu numărul înscris deasupra cuvântului respectiv.

Obținem astfel informația, ALAN TURING, ENIGMA, fiind deci vorba de matematicianul englez cu acest nume, specialist în logica matematică şi precursor al calculatoarelor electronice, unul dintre cei mai importanți membrii ai grupului de criptoanalişti englezi de la Bletchley Park, care au „spart" maşina germană de cifrat, botezată „ENIGMA".

În textul care urmează este disimulat numele unui român vestit, onorat cu titlul de „om al şcolii":

„Şcoala şi copiii românilor îi erau bucuria. Era un om hotărât şi găsea mereu resurse pentru pregătirea celor tineri."

Folosind acelaşi procedeu de disimulare, în următorul text este ascuns numele celui care i-a dedicat frumoasa poezie pe care o redăm. Textul este următorul: **„Cu un scop foarte sincer căutăm slujbe mai uşoare şi comode."**

Poezia este următoarea:

„Pe nouă să-l împarți la trei
Şi-apo la cub ridică suma
Atâtea luni să stai de-acuma
La locul hotărât de zei.

Iar Zeus, supremul geometru

Să-şi dea puteri să biruieşti

Ca-n sfera vieții româneşti

Nu arc să fii ci diametru.”

Informațiile suplimentare oferite, asigură succesul rezolvării, mai ales că dispunem de două texte în care s-a folosit acelaşi procedeu de disimulare.

Se găseşte astfel numele lui SPIRU HARET, primul român doctor în matematică (1878), fost ministru al instrucțiunii publice, contribuind decisiv la clădirea a peste 2000 de localuri de şcoli, înființând 1700 de posturi de învățători şi sporind astfel numărul ştiitorilor de carte din vechea România de la 22 la sută la 39 la sută.

Cel care i-a dedicat poezia este George Coşbuc.

Următorul exercițiu este dificil de soluționat, dar cu siguranță că tenacitatea şi intuiția vor învinge.

„Străduieştete să dai examenele restante. Am auzit că restanțierii obțin sigur aprobări pentru reeşalonarea susținerii, dacă sunt în regim internat. Toate universitățile stau prost financiar şi continuă să majoreze taxele, adun-nd astfel toate sumele de la studenții restanțieri. Tarifele precizate sunt deplin justificate, dar rămân exagerate.

Am plătit abonamentul la Vodafone.”

Disimularea informației se bazează pe două chei şi anume:

- Din ultimul cuvânt al textului, respectiv, VODAFON, înlocuind literele cu rangurile lor din alfabet, obținem următoarea secvență numerică, 2 2 1 5 4 1 6 1 5 1 4.

- Se rețin primele trei litere din primul cuvânt al textului, respectiv, S, T, R.

Din text se reţin cuvintele care urmează, după fiecare cuvânt care începe cu una dintre literele, S, T, R, deasupra acestor cuvinte se scrie, cifră cu cifră, secvenţa numerică de mai sus, repetând-o dacă este nevoie, şi din fiecare astfel de cuvânt extragem litera care, în cadrul lui, ocupă locul identic cu numărul înscris deasupra cuvântului.

Astfel:

2	2	1	5	4	....
Dai,	am,	obţin,	aprobări,	susţineri,	...

Literele astfel extrase formează informaţia, **„AM OBŢINUT CODURILE”**, având semnificaţia cunoscută de corespondenţi.

Un exerciţiu simplu care, prin textul care urmează, ne aminteşte numele unui vestit cărturar român:

„A dat mult acestui popor. Prin ideile avansate a impus Occidentului, contribuţia acestui intelogent popor, stima şi interesele sale. Erudit, cu pregătire deosebită, comparabil cu învăţaţii epocii, pildă de creator pentru români.”

Se consideră cuvintele de ranguri pare, grupate câte trei cuvinte consecutive şi în fiecare grupă, din primul cuvânt extragem prima literă, din al doilea cuvânt a doua literă iar din al treilea a treia literă. Literele astfel extrase formează secvenţa următoare: DCIAMNITTERMIIER.

Literele de ranguri pare conduc la numele, CANTEMIR, iar cele de ranguri impare dau numele, DIMITRIE, deci este vorba de DIMITRIE CANTEMIR (1673-1723), printre altele, membru al Academiei din Berlin.

Numele altui cărturar român este disimulat în textul următor:

„De luni până joi, inclusiv, sper să plec la munte, la răcoare. Poate mă voi duce cu Michel şi elevii şcolii sportive, care profită de zilele libere. Nu cred să-mi aprobe prelungirea sejurului."

Din zilele săptămânii, LUNI, MARȚI, MIERCURI, JOI, reținem numărul consoanelor, obținând secvența numerică, 2 3 4 1, pe care o scriem, cifră cu cifră, deasupra cuvintelor de ranguri pare, din textul care urmează după joi, şi din fiecare cuvânt extragem litera care, în cadrul lui are rangul identic cu numărul înscris deasupra cuvântului. Secvența numerică de mai sus, 2 3 4 1 se repetă de câte ori este nevoie.

Literele astfel extrase formează numele, PETRACHE POENARU (1799-1875), discipol al lui Gheorghe Lazăr, cu merite deosebite în organizarea învățământului național. În 1827 a brevetat la Paris intervenția tocului rezervor, cu piston.

Să presupunem că un cetățean primeşte de la un amic, următorul bilet:

Ca să te distrezi, îți trimit un text pe care să-l analizezi şi să găseşti în el titlul unui ziar, apărut sub conducerea lui Kogălniceanu.

Dar iată textul:

„În zilele de 12 şi 13, s-a planificat atestarea elementelor experimentate, viitori analişti. Verificarea unora poate să amăgească, dar rămân studenții capabili. Nu ne-a lăsat nici rectorul să primim numai integralişti. Te pup!"

Şi destinatarul s-a conformat.

A luat cuvintele de ranguri impare, începând cu primul cuvânt aflat după numărul 13, şi a scris deasupra lor, cifră cu cifră, numerele din secvența, 1213, formată din cele două numere, repetând-o de câte ori este necesar adică:

1	2	1	3	...
s-a	atestarea	experimentate	analiştii	...

şi din fiecare cuvânt a extras litera care, în cadrul lui, ocupă locul indicat de numărul înscris deasupra cuvântului respectiv.

Obține astfel numele ziarului, STEAUA DUNĂRII, ziar unionist apărut sub conducerea lui M. Kogălniceanu la Iaşi în perioadele 1855-1856 şi 1858-1860, dar şi la Bruxelles între 1856-1859.

Dar pentru un investigator tenace, rezultatul de mai sus se dovedeşte o cursă, o acoperire a adevăratei informații transmise.

El a luat formula de încheiere, TE PUP şi a înlocuit literele care substituie numerele, cu numerele respective, obținând secvența, 3414, pe care a scris-o, cifră cu cifră, deasupra cuvintelor de ranguri pare din text, extrăgând din fiecare cuvânt câte o literă, conform regulei anterioare.

Literele astfel extrase conduc la informația, „AM VIAGRA”, probabil că cei doi se ocupau cu comercializarea acestui produs.

În 1870, Eminescu trimite la Pesta, la ion Porțiu, trei articole în care, cu deosebită vigoare erau apărate drepturile românilor. După publicarea lor, Eminescu se alege cu un proces de presă, ca urmare a hotărârii Curții cu juri din Pesta.

Titlul unuia dintre aceste articole este înserat în următorul text:

„Articolele scrise au analizat cu rafinament şi autoritatea unui cercetător avizat, respectarea drepturilor majorității româneşti. Studiile publicate în Pesta constituie un prolog al numeroaselor atacuri, regretabile, fără realism, împotriva marelui poet Botoşănean.”

Titlul articolului este, „SĂ FACEM UN CONGRES” şi el a fost disimulat în text astfel:

Se consideră cuvântul EMINESCU, se înlocuieşte fiecare literă cu rangul ei din alfabet, 513914519321 şi elimin-nd numărul 9, rezultă cheia cu ajutorul căreia s-a ascuns în text titlul articolului, adică, 5131451321, care se scrie, cifră cu cifră, deasupra cuvintelor de ranguri pare din text, şi din fiecare cuvânt se extrage litera care ocupă rangul egal cu numărul înscris deasupra cuvântului respectiv.

În textul care urmează este ascunsă o informație care poate fi încadrată în traficul de influență:

„Câte amintiri avem cei care sărbătorim absolvirea. Monica nu recunoaşte că avea un loc privilegiat, curtată de fiul unui lider din academie.”

Primul cuvânt din text conduce la cheia folosită pentru ascunderea mesajului. Înlocuind literele acestui cuvânt, cu rangurile lor din alfabet şi eliminându-l pe zero, obținem cheia, 3125. Scriem numele ei, cifră cu cifră, deasupra cuvintelor de ranguri pare din text, şi din fiecare cuvânt extragem bigrama care începe cu litera care, în acel cuvânt, are acelaşi rang cu numărul înscris deasupra cuvântului respectiv. Literele astfel extrase formează informația căutată: **„ÎNCEARCĂ CU AVOCATUL LICĂ”.**

Exemplul care urmează ne arată că şi un înscris găsit într-un caz de suicid, trebuie analizat cu atenție. Iată textul:

„**Am decis să-mi nesocotesc norocul, am făcut zadarnică pregătirea, totul. Dacă mie frică rămân ridicol, aşa, ADIO!”**

Analiza atentă dezvăluie cauza acțiunii respectivului. În cuvântul ADIO, înlocuim literele cu rangurile lor din alfabet, şi renunțând la numărul nouă, obținem secvența, 1415, pe care o scriem în mod repetat deasupra

tuturor cuvintelor textului, începând cu al doilea, aceste numere arată care litere din cuvânt se extrag, litere care conduc la expresia, „**DIN CAUZA TA MARIA.”**

Din analiza textului care urmează, aflați numele celui care i-a schimbat numelui marelui nostru poet, din Eminovici în Eminescu:

„Nu contează că visul poetului avea sfințenia iubirii, soarta-l poate infirma.”

Şi dacă ați aflat cheia corectă, următorul text conține numele revistei condusă de cel înpricinat: **„Fetele măritate târziu, copil minunat nasc.”**

Suntem în cazul deținerii unor infoemații ajutătoare, precum şi a două texte în care informațiile au fost ascunse folosindu-se aceeaşi cheie, deci exercițiul are puține şanse să rămână fără rezolvare.

Cheia de disimulare este formată din secvența numerică 1615522112, repetată dacă este nevoie, şi obținută din cuvântul POETUL, înlocuind literele cu rangurile lor din alfabet, şi eliminând pe zero.

Acest şir se scrie, cifră cu cifră, deasupra tuturor cuvintelor din ambele texte, din fiecare cuvânt extrăgând litera care, în cadrul lui, ocupă rangul identic cu numărul înscris deasupra cuvântului respectiv.
Din primul text rezultă secvența, NACLUVFISOI, care citită de la dreapta conduce la numele căutat, IOSIF VULCAN, iar din al doilea text rezultă numele revistei, FAMILIA.

Prin următorul text se transmite un loc de întâlnire, pe care se cere să-l aflați:

„Nu te mai învinovății prosteşte, ai salvat un individ dominat sufleteşte, aflat la marginea prăpastiei, delirând.”

Scriem primii opt termeni din şirul lui Fibonacci, 1, 2, 3, 5, 8, 13, 21, 34, după care eliminăm separația dintre termeni, obținând un şir format

din 11 numere, 12358132134 pe care-l scriem, termen cu termen, deasupra tuturor cuvintelor textului şi din fiecare cuvânt extragem litera care ocupă locul indicat de numărul înscris deasupra cuvântului. Literele extrase formează expresia **„NE ÎNTÂLNIM LA ARAD.”**

O altă metodă de ascundere a unei informații într-un text, apare în următorul exemplu:

„Doresc o muzică fără motive populare, una săltăreață. Asistă crema artiştilor. Foloseşte instrumente reprezentative Ardealului, produc impresie intensivă. Voi închiria cinematograful Arta.”

Expresia de la început, „Doresc o muzică”, îi indică destinatarului de unde să formeze cheia. Din primul cuvânt reține denumirile celor două note muzicale, DO RE, din care, înlocuind literele cu rangurile lor din alfabet, obținem secvența, 415185, pe care o scriem, cifră cu cifră, deasupra tuturor cuvintelor, începând cu al patrulea, numărul înscris deasupra cuvântului arată a câta literă din el se reține.

Literele reținute formează expresia, „**AM LUAT MAŞINA DIN VAMĂ.”**

Scurte considerații privind cifrurile de substituție

În orice limbă, având un alfabet format din N litere, un text (sau mesaj) este o succesiune de litere, bigrame, ..., cuvinte, exppresii, pe care le numim elemente generatoare ale mesajelor. „Succesiunea” se supune unor legități, care sunt specifice fiecărei limbi.

Să considerăm cazul în care, elementele generatoare (sau elementele clare) sunt literele.

Dacă fiecare literă dintr-un mesaj, se înlocuieşte (se substituie) cu o altă literă, cu un număr, simbol, sau combinații ale acestora, spunemcă mesajul, sau textul, a fost cifrat cu un cifru de substituție, de litere, cu reprezentări unice. Din mesaj rezultă astfel o criptogramă, care, prin decriptare ne întoarce la mesaj.

În general, aceste substituții simple nu modifică legitățile, sau caracteristicile, statistice ale mesajelor, ele transferându-se criptogramei, şi tocmai această constatare stă la baza decriptării criptogramelor realizate cu aceste sisteme.

Dar să considerăm mai bine un exemplu.

Să se decripteze următoarea criptogramă:

OFPMOAFHPMF NKZSCVFNMM UDSN FOPAKC IK TNSGCKEK KOPK IKSOKGMPF

Criptograma are 54 de litere, care apar în ea cu următoarele frecvențe:

litere	A	C	D	E	F	G	H	I	K	M	N	O	P	S	T	U	V	Z
frecvențe	2	3	1	1	6	2	1	2	9	5	4	5	5	4	1	1	1	1

Vom nota literele mesajului, sau literele clare, cu caractere cursive.

În criptogramă cele mai frecvente litere sunt, k, f urmate de M, O, P, cu acelaşi număr de apariţii. În limba română, cele mai frecvente litere sunt, A, I, E, R, dar ordinea acestora este, în general, variabilă.

Deci literele din criptogramă, K, F, M, ar putea reprezenta literele clare, „a”, „i”, „e”, într-o anumită ordine.

Cea mai frecventă literă finală, a „cuvintelor” din criptogramă este K, iar cea mai frecventă literă finală de cuvinte în limba română este „e”, deci foarte probabil, din aceste două observaţii, că litera K din criptogramă, reprezintă litera clară „e”, fapt pe care-l notăm astfel, K=e. Al doilea „cuvânt” din criptogramă are în final litera M dublată, cum în limba română cel mai frecvent în final se dublează litera „i” rezultă că M=i şi atunci din prima constatare, a rămas că F=a.

În baza celor de mai sus, al şaptelea „cuvânt” din criptogramă devine,

K O P K

e . . e

dar cel mai frecvent cuvânt cu această structură este cuvântul „este” şi deci O=s şi P=t.

Din cele de mai sus rezultă că primul cuvânt devine:

O F P M O A F H P M F

s a t i s . a . t i a

care este cuvântul „satisfacţia”, şi deci, A=f şi H=c, după care decriptarea nu mai ridică probleme, ajungându-se la textul clar **„Satisfacţia rezolvării unor astfel de probleme este deosebită.”**

Şi acum încercaţi-vă forţele decriptând următoarele două criptograme, rezultatele se găsesc în finalul acestui capitol:

Exercițiul 1:

PM FO HA LF UFH HM MP RO IA MP FP IA EF LFN LC HFKA LA TF UFHA OFKA

Exercițiul 2

IZI B XZNL I ZALDB LBMXFDVXO ZD XVDOXO MXFIL

Dar lucrurile nu sunt întotdeauna atât de simple, deoarece există numeroase procedee prin care, criptogramele realizate cu aceste substituții simple de litere, să „opună” o rezistență mai mare la decriptare. Dintre acestea amintim următoarele:

- împărțirea arbitrară pe „cuvinte” a criptogramei, deci fără a respecta împărțirea pe cuvinte a textului clar.
- introducerea unor non-valori, deci unele litere sau numere „în plus”, care nu fac parte din criptograma reală,
- scrierea textului în sens invers, sau numai a unora dintre cuvintele lui şi numai după aceea se efectuează cifrarea etc.

Cel care efectuează cifrarea va trebui să găsească aceste „anomalii”, să le înlăture şi apoi să treacă la analiza criptogramei rămase.

Să vedem unu, sau două exemple.

Să se decripteze următoarea criptogramă:

AVDUV ITETB CDLBU XIBTC XIDDO SILLZ GLSNZ TMDBM AIXDL RBITW NBUVG TUVDO DNBDX SGBXZ IDCLB IDBBQ

Criptograma are 80 de litere, din care 20 sunt distincte, valoare care este mare, deoarece pentru un text de 80 de litere în limba română, numărul mediu al literelor distincte este aproximativ 16, deci este foarte probabil ca, în criptograma reală să fi fost introduse litere în plus, după o anumită regulă. Se mai constată că literele, O, Q, W şi Z apar numai la finalul grupelor de câte 5 litere, deci probabil că în aceste locuri au fost introduse aceste non-valori. Vom analiza aceste grupe.

În grupa întâi, AVDUV, observăm următoarele; suma rangurilor din alfabet ale primelor patru litere este egală cu, 1+22+4+21=48, număr care, modulo 26 (deci restul împărțirii lui la 26) este egal cu 22, rangul din alfabet al literei V, care apare în finalul acestei grupe.

Pentru grupa a doua, suma rangurilor din alfabet ale primelor patru litere, este egală cu 54 = 26x2+2, deci restul împărțirii lui 54 la 26 este egal cu 2, care este randul din alfabet al literei B, care apare în finalul acestei grupe.

Cercetând toate grupele din criptogramă, se confirmă regula de mai sus de obținere a literelor folosite drept non-valori, care au fost introduse după fiecare patru litere din criptograma reală.

Eliminăm toate literele din finalul grupelor şi analizăm criptograma rămasă, pentru care frecvențele literelor sunt următoarele:

A	B	C	D	E	G	I	L	M	N	R	S	T	U	V	X
2	9	2	11	1	2	8	5	1	3	1	3	6	3	3	4

cele mai frecvente fiind, în ordine descrescătoare, D, B, I, T, L, ... printre ele găsindu-se acelea care substituie cele mai frecvente litere din limba română, adică, a, e, i, t, n, r, o, ... Se poate acum continua prin încercări, mai indicată fiind calea studierii cu atenție a criptogramei.

Astfel, observăm că în criptogramă litera D apare de două ori dublată, în secvența IDD, respectiv, VDD şi cum în limba română, litera „i” se dublează cel mai frecvent, putem presupune că D din criptogramă reprezintă litera clară „i”, deci D=i, cu toate că nu se exclude posibilitatea ca, în cele două secvențe de mai sus, prima literă D să fie finala unui cuvânt, iar a doua să fie inițiala cuvântului care urmează în text.

Începând cu a 12-a literă din criptogramă, apare secvența BXIB, pe care o presupunem, pe baza frecvențelor acestor litere din criptogramă, că reprezintă secvența clară „este” de unde ar rezulta că, B=e; X=s şi I=t, urmând să răspândim aceste echivalări în criptogramă, pentru a le confirma, sau infirma.

Începând cu a 17-a literă din criptogramă, avem secvența,

X	I	D	D	S	I	L
S	t	i	i	.	t	.

care poate reprezenta cuvântul „ştiința”, deoarece litera L are o frecvență mare în criptogramă şi ar putea reprezenta litera clară „a” şi deci L=a.

Din aproape în aproape ajungem la textul clar:

„Criptologia este o ştiință având obiect şi metode proprii de investigație.”

Exerciții date spre rezolvare:

Exercițiul nr. 3

Să se decripteze criptograma:

HAIDZ DVPLD NREGL VSOVP LVHDD CGBNP GRYDS WVDPH AIRBT EVADR VSVOP VLRAS GDKBD

Exercițiul nr. 4

Să se descipteze criptograma următoare, textul clar fiind în limba franceză:

GFHVKV IFDFRETZVI ACFLIERCZJKVVK TIZKZHJLV RERKFCEV WIREGTV UVSLKMV VEG CEZKKVIRKLIV GIRI UVJL HJVIJ GRIEGRJJZVEJ

Exercițiul nr. 5

Să se decripteze următoarea criptogramă, textul clar fiind în limba engleză:

DDOLU CAOL CDHY BVM DAYVF EIYVRL CVBA CAOL EXBLLU BVM DAOL GHTHGVUZ HNLAOLYLK BHU DHYTF CHUK GTHYJOLK BAV DOLSW CAOL GAYVQHUZ

Dar lucrurile se mai pot complica atunci când trecem la substituțiille multiple, caracterizate prin aceea că, fiecare literă are mai multe reprezentări cifrante formate din litere, numere sau combinații ale acestora.

Dintre aceste sisteme, cele mai des folosite au fost cifrurile polialfabetice.

Să considerăm alfabetul normal ordonat (sau alfabetul clar), sub care scriem două sau mai multe, permutări ale sale, pe care le numim alfabete de cifrare, sau cifrante:

alfabet clar	A	B	C	D	E	...	Z
alf. de cif. 1	C	L	U	M	N	...	E
alf. de cif. 2	D	R	S	T	U	...	F

Pentru a cifra un text cu un astfel de sistem avem nevoie de o cheie de cifrare, care este o succesiune formată din numerele de ordine ale alfabetelor

de cifre, sau o permutare a acestora, cheie ale cărei numere se înscriu repetat deasupra literelor textului clar. Numărul înscris deasupra unei litere, indică din care alfabet se ia reprezentarea cifrantă a literei respective.

Astfel, dacă avem cinci alfabete de cifrare, cheia este succesiunea (12345), sau (31423) etc.

De exemplu, folosind schema anterioară cu două alfabete de cifrare şi cheia (12), cuvântul BADEA se cifrează astfel:

1	2	1	2	1
B	A	D	E	A
L	D	M	U	C

Cel care încearcă să cripteze o criptogramă realizată cu un astfel de sistem, va trebui ca pentru început să determine lungimea cheii de cifrare, deci implicit numărul alfabetelor de cifrare, după care scrie pe coloane (sau linii) toate literele care au fost cifrate cu acelaşi alfabet, deci fiecare coloană este rezultatul cifrării cu o substituție simplă cu reprezentări unice şi deci reduce decriptarea substituției polialfabetice la decriptarea unui număr de substituții simple, număr egal cu cel al alfabetelor folosite.

Evident că unele complicații pot să fie introduse.

Să încercăm să decriptăm următoarea criptogramă:

PAYDCU CULIWDIDOVO EMDUXEDO NO MCAZDAOYOWADDUA DIONOKU WIA NIYEDMEDO CEXF MOVO BOPOBUDAOCU WO PUNBUYFOCUI WOCISOVAB RUCWIXO

Analiza ei ne conduce la următoarele constatări:

- criptograma are 109 litere, din care 51 sunt vocale şi 58 consoane, numărul aproape egal al acestora este o caracteristică a textelor clare redactate în limba română,

- literele finale de cuvinte sunt în procent de 86 la sută formate din vocale, aceasta fiind o altă caracteristică a textelor clare din limba română.

- dacă urmărim secvențele formate din cel puțin patru litere consecutive, din cuvintele criptogramei, se observă că aproximativ 51 la sută din literele criptogramei, formează succesiuni de forma „consoană-vocală”, aceasta fiind o altă caracteristică a limbii române.

Din aceste constatări rezultă că, sistemul de cifrare folosit are particularitatea că cifrează consoanele prin consoane şi vocalele prin vocale.

Dacă s-a folosit un cifru polialfabetic, cu „n” alfabete, atunci în criptogramă apar secvențe identice, despărțite de un număr de litere, proporțional cu „n”.

În criptograma dată, de la bigrama DO, inclusiv, până la bigrama DO, din finalul celui de-al treilea cuvânt, sunt 10 litere, unde 10=2x5.

De la secvența DAO din al cincilea cuvânt, până la aceeaşi secvență din al 11-lea cuvânt sunt 44 = 2x2x11 litere etc.

Din descompunerile în factori al distanțelor, factorul comun cel mai frecvent, ne dă chiar numărul alfabetelor folosite.

În exemplul nostru s-au folosit deci două alfabete. Scriem criptograma pe două linii, alternativ „sus-jos”, adică

P	Y	C	C	L	...
A	D	U	U	I	...

literele din prima linie provin din cifrarea cu primul alfabet, iar cele din a doua linie, cu al doilea alfabet, deci fiecare linie este rezultatul cifrării cu câte o substituție simplă cu reprezentări unice. Notăm alfabetele cu A(1)

respectiv A(2). Frecvențele literelor din cele două linii, deci corespunzătoare celor două alfabete, sunt:

litere	A	B	C	D	E	F	I	K	L	M	N	O	P	R	S	U	V	W	X	Y	Z
A(1)	3	6	3	3	2	5	1	1	2	14	2	1	5	3	3	1					
A(2)	5	4	2	9	2	3	1	3	2	5	1	1	6	3	3	3	1				

Să ne imaginăm că deasupra literelor criptogramei am scris în mod repetat secvența (1 2), precizând astfel pentru fiecare literă din care alfabet provine.

În analiza care urmează, ținem cont de faptul că, vocalele sunt cifrate tot prin vocale şi consoanele prin consoane.

Astfel, pe primul alfabet, cea mai frecventă literă este O, care cade pe alfabetul unu, ca finală în cuvintele de ranguri, 2, 3, 4, 8, 10 şi 15, fiind cea mai frecventă literă finală de cuvinte, deci cu siguranță litera O din primul alfabet reprezintă litera clară „e”, fapt notat astfel, O(1)=e.

Dar atunci cuvântul scurt NO, unde N este din alfabetul doi şi O din primul, reprezintă cuvântul clar „de” şi deci N(2)=d.

De această manieră se continuă decriptarea, cititorul poate face acest lucru relativ uşor, ajungând la următorul text clar:

„Dintre rezultatele obținute de criptoanaliştii suedezi, mai cunoscute sunt cele referitoare la desciptarea mesajelor germane”.

Acest sistem este identic cu cel propus de ing. Ioan I. Oproiu, în lucrarea sa, „Carnetul criptografic pentru corespondența secretă”, brevetat cu nr. 4742, la 29 octombrie 1919 şi tipărit la Piatra-Neamț.

Autorul şi-a prezentat intervenția astfel: „Corespondena secretă prin ajutorul acestui carnet poate fi întrebuințată cu folos în afaceri comerciale, industriale, afaceri de bursă, afaceri de familie cu caracter secret, în armată,

în poliția secretă. **Acest carnet constituie ultima şi cea mai completă perfecționare a corespondenței secrete prin ajutorul criptografiei."**

După cum o demostrează, şi exemplul tratat de noi mai sus, erorile de concepție ne îndreptățesc să afirmăm că, I. Oproiu s-a grăbit atunci când şi-a apreciat sistemul cu atâta optimism.

Dar următoarele constatări rezultate din această apariție editorială, merită a fi reținute:

- prin legislația existentă în țara noastră la 1919, preocupările de criptologie erau sprijinite şi protejate de stat, dovadă stă brevetul acordat autorului,

- se pare însă că, la momentul respectiv, statul nu dispunea de un grup de specialişti criptologi, care să fie consultați în astfel de probleme, altfel nu se explică acrodarea brevetului pentru un sistem atât de vulnerabil la decriptare.

Ca fapt divers amintim că, principiul cifrării consoanelor prin consoane şi vocalelor prin vocale, a fost aplicat de japonezi la unele maşini de cifrat, folosite în al doilea război mondial, maşini devenite „victime" ale criptoanaliştilor germani şi americani.

Şi acum încercați-vă forțele:

Exercițiul nr. 6

Să se decripteze următoarea criptogramă:

UC EGEMM XFBDMDXOM UKMJWQX BZUHDBTFXVQ HMHINX HB ETVFDKGA IMGMUNXPK MJ YMRNF UKACM ODFGC WMIX RXBZS WUUBOJEFPMUAX UC LFDIMGXM UXZDFQCNXJB EX VACLQRBZIXXT NZTHDX WQOTEIKAPLQ PEQ GXGHBFTEAG BZUKMRMAGBXDK

Exercițiul nr. 7

Să se decripteze următoarea criptogramă, ştiind că a fost cifrată şi pauza (sau spațiul) dintre cuvinte:

WETJL CUNTP BBECT UZJUE GIMJM PFWYR SEXXB
JZBSS XCMED VBASN PPBBE CVMZX XBAEB SEEXR
PAIBH MBAEB DVTOS YIYWF XLGMT FWLAI BTPBT
VLFYY FTCXR NXTPF EWFPF CSCTM BRECT UNJRZ
HXPPU WJQPP UDXUE DEETU CDWEJ VTAIB TMBFU

Acestea au fest cele câteva probleme referitoare la criptologie pe care am dorit să le prezentăm.

Dacă ele par puțin plicticoase, vă prezentăm câteva probleme de divertisment – criptologic, având tangență cu mult mediatizata numerologie, despre care Martin Gardner, în cartea sa „Amuzamente matematice”, Ed. Ştiințifică 1986, afirmă că nu este altceva decât un amuzament matematic, care presupune imaginație, perseverență, spirit iscoditor, inventivitate şi creativitate, deci – adăugăm noi – calități absolut necesare tuturor celor preocupați de cercetarea ştiințifică şi implicit de criptologie.

În matematică sunt cunoscute aşa – numitele NUMERE PRIETENE, acestea fiind două numere, n şi M având proprietatea că, suma divizorilor (sau părților) numărului N este egală cu M, şi suma divizorilor lui M este egală cu N.

Prima pereche de numere prietene, şi anume perechea formată din 220 şi 284, a fost pusă în evidență de Pitagora. Divizorii lui 220 sunt: 1, 2, 4, 5, 10, 20, 11, 22, 44, 55, 110 iar suma lor este egală cu 284. Divizorii lui 284 sunt: 1, 2, 4, 71, 142 iar suma lor este egală cu 220.

Se presupune că, pornind de la proprietatea unei astfel de perechi, Pitagora a dat cea mai profundă definiție prieteniei:

„Doi oameni sunt cu adevărat prieteni dacă se comportă ca numerele 220 şi 284, adică toate gândurile, toate aspirațiile, toate preocupările unuia să aibă sălaş în sufletul celuilalt.”

În ordine cronologică, perechile de numere prietene au fost descoperite de Pitagora (220 şi 284), Fermat (17296 şi 18416), Descartes (9363584; 9437056) şi marele matematician Euler, care a pus în evidență 59 de perechi de astfel de numere.

O primă constatare; numele celor patru matematicieni, au în comun numai litera R, al cărei rang în alfabet este egal cu 18.

Dar, (220+284) = 18x28 unde 28 este număr „perfect” căci suma divizorilor lui, adică, 1, 2, 4, 7, 14, este egală cu 28.

Relația obținută mai sus, ar putea fi interpretată astfel;

„începând cu Pitagora (în partea stângă a relației se afla suma celor două numere descoperite de el), cercetările celor patru matematicieni referitoare la numerele prietene, s-au derulat sub semnul perfecțiunii.”

Să considerăm următoarea substituție simplă, cu reprezentări unice:

A	B	C	...	P	Q	R	S	T	...	Z
10	11	12	...	25	26	1	2	3	...	9

cu ajutorul căreia cifrăm numele celor patru matematicieni, şi pentru fiecare caz în parte calculăm suma reprezentărilor cifrate.

Astfel, pentru primul nume avem:

P	I	T	A	G	O	R	A
25	18	3	10	16	24	1	10

cu suma reprezentărilor, 25 + 18 + 3 + 10 + 16 + 24 + 1 + 10 = 107

Pentru Fermat, suma reprezentărilor este 65, pentru Descartes suma este 71, iar pentru Euler, suma reprezentăriloe este 54.

Ponderând primele trei sume de mai sus cu numerele care exprimă locul ocupat de fiecare matematician în cronologia acestor preocupări (Pitagora – primul, Fermat – al doilea şi Descartes al treilea, obținem, 1 x 107 + 2 x 65 + 3 x 71 = 450, la care, dacă adunăm suma obținută pentru Euler, se obține, 450 + 54 = 504 = (220 + 284).

Iată deci că preocuparea comună a celor patru pentru numerele prietene are o motivație şi susținere ... logică, fapt obținut cu ajutorul unei substituții.

Dacă ponderăm şi suma obținută pentru euler, obținem 450 + 4 + 54 = 666, număr considerat în numerologie număr divin sau „numărul fiarei”,pe care , în acest caz, îl vom considera ca suport al afirmației că cei patru reprezintă „monştrii sacrii” ai preocupărilor pentru progresul general al cunoaşterii umane.

Să considerăm următoarea substituție:

A	B	C	D	E	...	X	Y	Z
25	26	27	28	29	...	48	49	50

cu care cifrăm cuvântul NUMERE şi adunăm reprezentările cifrate adică

N	U	M	E	R	E
38	45	37	29	42	29

deci, 38 + 45 + 37 + 29 + 42 + 29 = 220.

Facem acelaşi lucru pentru cuvântul PRIETENE şi obținem că suma reprezentărilor cifrate este egală cu 284.

În acest fel, cu ajutorul substituției, perechea de cuvinte (numere prietene) a fost pusă în corespondență cu perechea de numere, (220, 284), deci alegerea numelui pentru astfel de numere nu este întâmplătoare.

Următoarea întâmplare vine să confirme ... matematic prietenia dintre Eminescu şi Veronica Micle.

Lungimile în litere ale numerelor, EMINESCU şi VERONICA, sunt egale cu 8. Considerăm substituția,

A	B	C	D	...	X	Y	Z
8	9	10	11	...	31	32	33

cu ajutorul căreia cifrăm numele celor doi apropiați. Astfel,

M	I	H	A	I		E	M	I	N	E	S	C	U
20	16	15	8	16		12	20	16	21	12	26	10	28

V	E	R	O	N	I	C	A		M	I	C	L	E
29	12	25	22	21	16	10	8		20	16	10	19	12

se constată că, pentru fiecare caz în parte, suma reprezentărilor cifrate este egală cu 220.

În fiecare dintre cele două nume, Eminescu şi Veronica, numărul vocalelor este egal cu cel al consoanelor, fiind câte 4 din fiecare.

Vom considera atunci următoarea substituție:

A	B	C	....	X	Y	Z
4	6	8	...	50	52	54

cu care vom cifra numele celor doi, şi vom calcula suma reprezentărilor cifrante. Se constată că, pentru fiecare caz în parte, suma reprezentărilor cifrante este egală cu 284.

Am reuşit astfel, ca prin acest procedeu criptologic să punem în corespondență perechea, (Eminescu, Veronica) cu perechea de numere prietene (220, 284) şi dacă ne gândim la definiția dată prieteniei de Pitagora, din cele de mai sus rezultă .... matematic că cei doi au fost cu adevărat prieteni.

Soluțiile problemelor propuse:

Exercițiul 1.

Este vorba de o substituție simplă, textul clar fiind următorul: **„Nu am ce să fac cu un om de un an, de la sat, şi care se va face mare.”**

Exercițiul 2.

Textul clar: **„Aşa e uşor a scrie renumitul şi utilul număr”.**

Dacă înlocuim fiecare cuvânt cu numărul literelor sale, şi după primul număr scriem virgula se obține numărul PI, cu 8 zecimale adică, 3, 14 15 9 2 6 5.

Exercițiul 3.

O substituție simplă în care pauza dintre cuvinte s-a notat cu litera Q, fiind şi ea cifrată şi s-au introdus în criptogramă non-valori după următorul criteriu, după fiecare două litere din criptogramă s-a introdus o a treia, al cărei rang în alfabet este suma modulo 26 a rangurilor celor două litere precedente. Se elimină aceste litere şi se ajunge la mesajul: **„Un q mic q artificiu q etc.”**

Exercițiul 4.

Şi această criptogramă conține non-valori. După ce s-a cifrat primul cuv)nt, se obține, GFVKV, litera de rang minim este F, având rangul 6, la care se adună 2, rezultând numărul 8 care este rangul lui H, şi după F scriem litera H. Aşa se procedează pentru toate cuvintele.

Se obține textul clar: **„Poète, romancier journaliste et critique, Anatole france débute en littérature per des vers parnassiens.”**

Exercițiul 5.

Şi această criptogramă conține non-valori, care ocupă primul loc în fiecare cuvânt al criptogramei, aceste litere au fost introduse după următorul procedeu: din numărul de cuvinte al grupei se scade o unitate, numărul obținut este rangul literei false care se scrie pe primul loc al „cuvântului" din criptogramă.

Textul clar este: **„When the war of troy broke out the Queen of the amazons Gethered an army and marched to help the trojans."**

Exercițiul 6.

Este un cifru polialfabetic folosind trei alfabete de cifrare.

Textul clar este: **„În lupta împotriva fraudei informatice statul şi sectorul particular au făcut front comune date fiind dificultățile în stoparea fenomenului şi consecințele uneori dezastruoase ale reuşitelor infractorilor."**

Exercițiul 7.

Tot o substituție folosind trei alfabete.

Textul clar este: **„Ştefan cel Mare nu trebuie socotit un domnitor local mărginit la datinile şi la orizontul țării sale, el era un principe al Europei care cunoştea lumea şi toate rosturile ei."**

Bibliografie:

1. David Kahn, „The Codebreakers. The story of secret writing” New York, 1976
2. R. V. Iones, „ Un război ultrasecret”, Ed. Pol. Bucureşti, 1983
3. V. P. Borovicka „Cifruri strict secrete”, Ed. Pol. Bucureşti, 1984
4. F. Constantiniu, ‚Enigma şi alte enigme”, Almanahul Oştirii” 1987, pag. 92-94.
5. E. Nicolaescu „Rebus şi criptologie”, Rebus, nr. 423 şi 424 1975
6. I. Torsan „Asupra energiei informaționale”, Studii şi Cercetări Matematice, Ed. Academiei Române, tom. 25/1973
7. I. Torsan, „Unele considerații pe marginea confruntărilor criptologice în cel de-al doilea război mondial”, Rev. Acad. Tehn. Militare, nr. 2/1993
8. I. Cristescu, I Torsan „Probleme de criptografie”, Anal. Univ. Bucureşti, matem. mec. Nr. 1973
9. I. Torsan „Criptologia – artă a conversației secrete” Rev. Pentru Patrie, nr. 10, 11, 12 din 1993 şi nr. 1, 2, 3 din 1994
10. I. Torsan, „Mari matematicieni – experți criptologi” Rev. Frontiera, nr. 7, 8, 9, 10 din 1993
11. I. Torsan, „Considerații privitoare la utilitatea scrierii istoriei criptologiei din România” Rev. „Cele trei crişuri”, Oradea, Seria a III-a, anul I, nr. 10-12, anul 2000.